Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1

16-300698
Issue 7
November 2009

© 2009 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Hardware Documentation, Document number 03-600759.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

http://www.avaya.com/support

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Software License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s):

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's Web site at:

http://support.avaya.com/ThirdPartyLicense/

Interference

Using a cell, mobile, or GSM telephone, or a two-way radio in close proximity to an Avaya IP Telephone might cause interference.

Security

See http://support.avaya.com/security to locate and/or report known vulnerabilities in Avaya products. See http://support.avaya.com to locate the latest software patches and upgrades. For information about secure configuration of equipment and mitigation of toll fraud threats, see the Avaya Toll Fraud and Security Handbook at http://support.avaya.com.

Contents

Chapter 1: Introduction 9
About This Guide 9
Change History 10
What's New in This Release. 10
Document Organization 12
Other Documentation 13

Chapter 2: Administration Overview and Requirements 15
9600 Series IP Telephones 15
Parameter Data Precedence 18
The Administrative Process. 18
Administrative Checklist 19
Telephone Initialization Process 20
Step 1: Telephone to Network 20
Step 2: DHCP Server to Telephone 21
Step 3: Telephone and File Server 21
Step 4: Telephone and the Call Server 21
Error Conditions 22

Chapter 3: Network Requirements 23
Network Assessment 23
Hardware Requirements. 23
Server Requirements 24
DHCP Server 24
HTTP/HTTPS Server 24
Web Server (Optional) 25
Required Network Information 25
Other Network Considerations 26
SNMP 26
Reliability and Performance. 27
QoS 27
IEEE 802.1D and 802.1Q 27
Network Audio Quality Display on 9600 Series IP Telephones 28
Qtest for Audio Quality 28
IP Address Lists and Station Number Portability 29
TCP/UDP Port Utilization 30
Security. 33
Registration and Authentication 34

Time-to-Service (TTS) 34

Chapter 4: Communication Manager Administration 37

Call Server Requirements 37
Switch Compatibility and Aliasing IP Telephones 37
Call Server (Switch) Administration 38
IP Interface and Addresses 39
UDP Port Selection 39
RSVP and RTCP/SRTCP 39
QoS 40
IEEE 802.1D and 802.1Q 40
NAT 40
DIFFSERV 41
Voice Mail Integration 41
9600 Series IP Telephones with CM 4.0+ Native Support 41
9600 Series IP Telephones Aliased as 4600 Series IP Telephones 41
Call Transfer Considerations 42
Conferencing Call Considerations 43
Telephone Administration 44
System-Wide Administration 44
Feature-Related System Parameters 44
Administering Stations 46
Aliasing 9600 Series IP Telephones 47
Administering Features 47
Feature Buttons and Call Appearances 48
For the 9610 IP Telephone 48
For the 9620/9620L/9620C IP Telephone 49
For 9630/9630G, 9640/9640G, 9650/9650C, and 9670G IP Telephones 49
Enhanced Phone Screen Display for 9630/9630G and 9640/9640G IP Telephones 51
9650/9650C Aux Button Assignments 51
Button Module(s) (SBM24) on the 9630/9630G, 9640/9640G, 9650/9650C, and 9670G 51
Conference Details Screen for Ad-Hoc Conferences 51
Special Considerations for the 9650/9650C IP Telephone 52
Special Considerations for the 9670G IP Telephone 53
Shuffling 53
Wide Band Codecs 54

Chapter 5: Server Administration 55
Software Checklist 55
DHCP and File Servers 55
DHCP Server Administration 56
Configuring DHCP for 9600 Series IP Telephones 56
DHCP Generic Setup 58
Windows NT 4.0 DHCP Server 63
Verifying the Installation of the DHCP Server 63
Creating a DHCP Scope for the IP Telephones 63
Editing Custom Options 64
Adding the DHCP Option 64
Activating the Leases 65
Verifying Your Configuration 65
Windows 2000 DHCP Server 66
Verifying the Installation of the DHCP Server 66
Adding DHCP Options 68
Activating the New Scope 69
HTTP Generic Setup 69
HTTP/HTTPS Configuration for Backup/Restore 70
For IIS Web Servers 70
For Apache Web Servers 77
Internal Audio Parameters 78

Chapter 6: Telephone Software and Application Files 79
General Download Process 79
9600 Series IP Telephone Scripts and Application Files 80
Choosing the Right Application File and Upgrade Script File 80
Upgrade Script File 80
Settings File 81
Contents of the Settings File 82
The GROUP System Value 83

Chapter 7: Administering Telephone Options 85
Administering Options for the 9600 Series IP Telephones 85
VLAN Considerations 100
VLAN Tagging 100
VLAN Detection 100
VLAN Default Value and Priority Tagging 101
VLAN Separation 102

DNS Addressing 103
IEEE 802.1X 104
802.1X Pass-Through and Proxy Logoff 105
802.1X Supplicant Operation 105
Link Layer Discovery Protocol (LLDP) 106
Local Administrative Options Using the Telephone Dialpad 111
Language Selection 112
Administering Voice-Initiated Dialing 113
Gigabit Ethernet Adapter 114
Dialing Methods 114
Log Digit (Smart Enbloc) Dialing 115
Enhanced Local Dialing 115
Enhanced Local Dialing Requirements. 117
Administering Features on Softkeys 117
Administering a Custom Screen Saver. 126
Backup/Restore 127
Backup 129
Restore 131
9610 Backup/Restore 132
9610 Retrieval Procedures 133
General 9610 Restore Processing 134

Chapter 8: Administering Applications and Options 137
Customizing 9600 Series IP Telephone Applications and Options. 137
The Application Status Flag (APPSTAT) 144
Special Administration for the 9610 145
Special Administration for the 9670G 145
Avaya "A" Menu Administration 146
Administering Phone Settings and Options and Settings (OPSTAT and OPSTAT2) 147
Main Avaya Menu with WML Applications Administered 148
Main Avaya Menu with Browser (Only) Administered. 149
Main Menu – No WML Applications Administered 150
Avaya Menu Administration With WML Applications 152
WML Application Display on the 9670G Home Screen 153
Sample Avaya Menu Administration File Template 158
Guest User Administration 160
Timer Operation for the 9620/9620L/9620C, 9630/9630G, 9640/9640G, 9650/9650C and 9670G. 160

Requirements for USB Devices 162
USB File/Device Support 162
Contacts File Format for USB Devices 162
USB Login Setup 163
USB Pictures 164

Chapter 9: Administering Specific 9600 Series IP Telephones 167
Introduction 167
Special Administration for the 9610 IP Telephone 167
General Functionality 167
Key 9610 Administration Concepts 168
Backup File Format 169
Main Menu (MM) Administration 170
Contacts Application Administration 171
The 9610 Idle Application, WMLIDLETIME, SCREENSAVERON, IDLEAPP, and WMLSMALL 171
9610 Craft Procedures 173
Troubleshooting a 9610 IP Telephone 173
Sample 9610data.txt File 174
Sample idle.wml File 176
Sample hotel.wml File 176

Appendix A: Glossary of Terms 177

Appendix B: Related Documentation 183
IETF Documents 183
ITU Documents 183
ISO/IEC, ANSI/IEEE Documents 183

Appendix C: Sample Administration Forms 185

Index 195

Chapter 1: Introduction

About This Guide

This guide is for personnel who administer Avaya Communication Manager, DHCP, HTTP/HTTPS servers for 9600 Series IP Telephones, a Local Area Network (LAN), or a Web server.

The 9600 Series IP Telephones use Internet Protocol (IP) technology with Ethernet line interfaces and support the H.323 protocol only. The 9600 Series IP Telephones provide support for DHCP, HTTP, and HTTPS over IPv4/UDP, which enhance the administration and servicing of the telephones. These telephones use DHCP to obtain dynamic IP Addresses, and HTTPS or HTTP to download new versions of software or customized settings for the telephones.

CAUTION:

Avaya does not support many of the products mentioned in this document. Take care to ensure that there is adequate technical support available for servers used with any 9600 Series IP Telephone system. If the servers are not functioning correctly, the 9600 Series IP Telephones might not operate correctly.

Note:

This guide covers administration of 9600 Series IP Telephones using H.323 protocol only. For information about administering these telephones in a Session Initiation Protocol (SIP) environment, see *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Administrator Guide* (Document Number 16-601944).

Important:

IP Telephone Software Release 3.1 does not support Avaya Communication Manager (CM) releases prior to 3.1.

Tip:

For a quick reference to Avaya Communication Manager settings for 9600 Series IP Telephones and related telephone interface information, see *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Read This First* (Document Number 16-601533), available at: www.avaya.com/support.

Change History

Issue 1	This document was issued for the first time in July 2006 to support the first release of 9600 Series IP Telephones.
Issue 2	This version of the document, revised and issued in September 2006, supports 9600 Series IP Telephone Software Release 1.1.
Issue 3	This version of the document was revised in January, 2007 to support 9600 Series IP Telephone Software Release 1.2.
Issue 4	This version of the document was revised and issued in May, 2007 to support Software Release 1.5.
Issue 5	This version of the document was revised and issued in May, 2008 to support 9600 Series IP Telephone Software Release 2.0.
Issue 6	This version of the document was revised and issued in February, 2009 to support 9600 Series IP Telephone Software Release 3.0 and the addition of three new telephone models: 9620L, 9620C, and 9650C. What's New in This Release describes Release 3.0 in more detail.
Issue 6	This version of the document was revised and issued in May, 2009 to support the addition of the 9670G telephone model, running on 9600 Series IP Telephone Software Release 2.0; this 9670-specific issue was concurrent with Issue 6 for Software Release 3.0.
Issue 7	This is the current version of this document, revised and issued in November, 2009 to support 9600 Series IP Telephone Software Release 3.1. In addition to software enhancements, this version incorporates the 9670G IP Telephone's administration requirements and information, previously issued separately in May, 2009. What's New in This Release describes Release 3.1 in more detail.

What's New in This Release

New material in this issue to support Release 3.0 software includes:

- Support for telephone administration and operation with Virtual Private Networks (VPNs). The *VPN Setup Guide for 9600 Series IP Telephones* (Document 16-602968) provides details about administering 9600 Series IP Telephones to enable users to access your network (call servers, file servers, etc.) through a VPN. In addition, a new local administrative (Craft) option has been added for VPN; this new Craft procedure is also described in the *VPN Setup Guide for 9600 Series IP Telephones* (Document 16-602968).
- Support for QTEST procedures such as adding the parameter QTESTRESPONDER. See Qtest for Audio Quality on page 28 for more information.
- Enhanced power management to save energy and expense, as follows:

  - Support for LLDP MED Extended Power-Via-MDI TLV, enabling the telephone backlight to use a minimum power level when On.
  - A "Backlight Off" softkey/icon can now be administered to allow the end user to turn off the telephone backlight for idle call states. See Administering Features on Softkeys for more information.

- All 96xx telephones except the 9610 now support Simple Certificate Enrollment Protocol (SCEP). The following new system parameters support this feature and have been added to the list of Customizeable System Parameters in Chapter 7 of the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide*: MYCERTRENEW, MYCERTURL, MYCERTKEYLEN, MYCERTCAID, MYCERTCN, MYCERTDN and SCEPPASSWORD.
- New system parameters DHCPSRVR (to specify DHCP server addresses) and GRATARP (to handle gratuitous ARPs) have been added to the list of Customizeable System Parameters in Chapter 7.
- The 9670G IP Telephone has been upgraded to include all software Release 3.0 and 3.1 enhancements, for example, the "LightOff" icon on its Home screen and the Edit Dialing feature. The 9670G must be aliased as a 9640, but does not require unique installation or administration. Administration enhancements related exclusively to the 9670G include:
  - new parameters WEATHERAPP and WORLDCLOCKAPP - allow to enable (the default) or disable presentation of a Weather or World Clock application on the 9670 Home screen.
  - specific icons for WML applications can be designated via the AvayaMenuAdmin.txt file. For more information, see Avaya "A" Menu Administration.
- Enhancements that have no impact on administration or installation include:
  - the Voice Dialing feature now accept audio input from an Avaya-approved headset, as well as from the telephone speaker.
  - users with access to Phone Settings have a new option called "Go to Phone Screen on Answer" that when enabled (the default) automatically displays the Phone screen when a call is answered.
  - several enhancements were added to help expedite failover to Local Survivable Processors (LSPs) in applicable scenarios.
- For the 9760G exclusively:
  - various minor enhancements have been made to the user interface.
  - the end user can designate up to 16 Favorites to display on the Home screen.

Document Organization

The guide contains the following sections:

Chapter 1: Introduction	Provides an overview of this document.
Chapter 2: Administration Overview and Requirements	Provides an overview of the administrative process and describes general hardware, software, and operational requirements.
Chapter 3: Network Requirements	Describes administrative requirements for your Local Area Network.
Chapter 4: Communication Manager Administration	Describes how to administer Avaya Communication Manager to operate with 9600 Series IP Telephones.
Chapter 5: Server Administration	Describes DHCP, TFTP, and HTTP/HTTPS administration for the 9600 Series IP Telephones.
Chapter 6: Telephone Software and Application Files	Describes telephone software, covers application software downloads, and provides information about the configuration file.
Chapter 7: Administering Telephone Options	Describes how to use file parameters and options to administer 9600 Series IP Telephones. Covers backup and restoration of telephone data. Also describes how to use local procedures to customize a single telephone from the dialpad.
Chapter 8: Administering Applications and Options	Provides a table of customizable application-specific parameters, to provide administrative control of telephone functions and options.
Chapter 9: Administering Specific 9600 Series IP Telephones	Covers special administration requirements for applicable 9600 Series IP Telephone models.
Appendix A: Glossary of Terms	Provides a glossary of terms used in this document or which can be applicable to 9600 Series IP Telephones.
Appendix B: Related Documentation	Provides references to external documents that relate to telephony in general, which can provide additional information about specific aspects of the telephones.
Appendix C: Sample Administration Forms	Provides examples of Avaya Communication Manager forms related to system wide and individual telephone administration.

Other Documentation

See the Avaya support site at http://www.avaya.com/support for 9600 Series IP Telephone technical and end user documentation.

See Appendix B: Related Documentation for information about accessing non-Avaya documents, such as those published by the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU).

For information about administering a virtual private network (VPN) for 9600 Series IP Telephones, see the *VPN Setup Guide for 9600 Series IP Telephones* (Document Number 16-602968), also available on the Avaya support site.

Chapter 2: Administration Overview and Requirements

9600 Series IP Telephones

All 9600 Series IP Telephones currently support the H.323 signaling protocol. The 9620, 9630, and 9640 can alternately be configured to support Session Initiation Protocol (SIP), as covered in the *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Administrator Guide* (Document Number 16-601944). This document covers only 9600 Series IP Telephones supporting H.323.

The H.323 standard provides for real time audio, video, and data communications transmission over a packet network. An H.323 telephone protocol stack comprises several protocols:

- H.225 for registration, admission, status (RAS), and call signaling,
- H.245 for control signaling,
- Real Time Transfer Protocol (RTP) and Secure Real Time Transfer Protocol (SRTP)
- Real Time Control Protocol (RTCP) and Secure Real Time Control Protocol (SRTCP)

The parameters under which the 9600 Series IP Telephones need to operate are summarized as follows:

- Telephone Administration on the Avaya Media Server, as covered in Chapter 4: Communication Manager Administration.
- IP Address management for the telephone, as covered in DHCP and File Servers on page 55 for dynamic addressing. For static addressing, see the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*.
- Tagging Control and VLAN administration for the telephone, if appropriate, as covered in Chapter 7: Administering Telephone Options.
- Quality of Service (QoS) administration for the telephone, if appropriate. QoS is covered in QoS on page 27 and QoS on page 40.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP).
- Interface administration for the telephone, as appropriate. Administer the telephone to LAN interface using the PHY1 parameter described in Chapter 3: Network Requirements. Administer the telephone to PC interface using the PHY2 parameter described in “Interface Control” in the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide.*
- Application-specific telephone administration, if appropriate, as described in Chapter 8: Administering Applications and Options. An example of application-specific data is Web-specific information required for this optional application.

Table 1 indicates that you can administer system parameters in a variety of ways and use a variety of delivery mechanisms like:

- Maintaining the information on the call server.
- Manually entering the information by means of the telephone dialpad.
- Administering the DHCP server.
- Editing the configuration file on the applicable HTTP or HTTPS file server.
- User modification of certain parameters, when given administrative permission to do so.

Note:

Not all parameters can be administered on all delivery mechanisms.

Table 1: Administration Alternatives and Options for 9600 Series IP Telephones

Parameter(s)	Administrative Mechanisms	For More Information See:
Telephone Administration	Avaya call server	Chapter 4: Communication Manager Administration, Chapter 5: Server Administration, and Appendix B: Related Documentation.
IP Addresses	DHCP (strongly recommended)	DHCP and File Servers on page 55, and especially DHCP Server Administration on page 56.
	Configuration file	Chapter 6: Telephone Software and Application Files and Chapter 7: Administering Telephone Options.
	Manual administration at the telephone	"Static Addressing Installation" in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide.*
	LLDP	Link Layer Discovery Protocol (LLDP) on page 106
Tagging and VLAN	LLDP	Link Layer Discovery Protocol (LLDP) on page 106.
	DHCP	DHCP Server Administration on page 56, and Chapter 7: Administering Telephone Options.
	Configuration file (strongly recommended)	DHCP and File Servers on page 55 and Chapter 7: Administering Telephone Options.
	Manual administration at the telephone	"Static Addressing Installation" in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

1 of 2

Table 1: Administration Alternatives and Options for 9600 Series IP Telephones (continued)

Parameter(s)	Administrative Mechanisms	For More Information See:
Quality of Service	Avaya call server (strongly recommended)	UDP Port Selection on page 39 and Appendix B: Related Documentation.
	DHCP	DHCP and File Servers on page 55, and Chapter 7: Administering Telephone Options.
	Configuration file	DHCP and File Servers on page 55, and Chapter 7: Administering Telephone Options.
Interface	DHCP	DHCP and File Servers on page 55, and Chapter 6: Telephone Software and Application Files.
	Configuration file (strongly recommended)	DHCP and File Servers on page 55, and Chapter 6: Telephone Software and Application Files.
	LLDP	Link Layer Discovery Protocol (LLDP) on page 106.
	Manual administration at the telephone	"Secondary Ethernet (Hub) Interface Enable/ Disable" in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.
Application - specific parameters	DHCP	DHCP and File Servers on page 55, and especially DHCP Server Administration on page 56. Also, Chapter 8: Administering Applications and Options.
	Configuration file (strongly recommended)	DHCP and File Servers on page 55, and especially HTTP Generic Setup on page 69. Also, Chapter 8: Administering Applications and Options.
VPN	DHCP	DHCP and File Servers on page 55, and Chapter 6: Telephone Software and Application Files. Also see the *VPN Setup Guide for 9600 Series IP Telephones* (Document 16-602968 for VPN details.
	Configuration file (strongly recommended)	*VPN Setup Guide for 9600 Series IP Telephones* (Document 16-602968).

2 of 2

General information about administering DHCP servers is covered in DHCP and File Servers on page 55, and more specifically, DHCP Server Administration on page 56. General information about administering HTTP servers is covered in DHCP and File Servers, and more specifically, HTTP Generic Setup. Once you are familiar with that material, you can administer telephone options as described in Chapter 7: Administering Telephone Options.

Parameter Data Precedence

If a given parameter is administered in multiple places, the last server to provide the parameter has precedence. The precedence, from lowest to highest, is:

1. LLDP,
2. Manual administration, with the two exceptions described for the system parameter STATIC on page 97,
3. DHCP, except as indicated in Table 9: DHCPACK Setting of System Values,
4. HTTP,
5. the Avaya Media Server, and finally,
6. Backup files, if administered and if permitted.

Settings the IP telephone receives from backup files or the file server overwrite any previous settings, including manual settings. The only exception to this sequence is in the case of VLAN IDs. In the case of VLAN IDs, LLDP settings of VLAN IDs are the absolute authority. Then the usual sequence applies through HTTP. If the VLAN ID after HTTP is not zero, any VLAN ID from the file server is ignored.

Note:

For the L2QVLAN and L2Q system values, LLDP settings of VLAN IDs are the absolute authority only if the LLDP task receives the VLAN IDs before DHCP and HTTP, and the DHCP client of the telephone is activated at all. If the LLDP task receives the VLAN IDs after DHCP negotiation, several criteria must be successful before the telephone accepts VLAN IDs from LLDP. For more information, see Link Layer Discovery Protocol (LLDP).

The Administrative Process

The following list depicts administration for a typical 9600 Series IP Telephone network. Your own configuration might differ depending on the servers and system you have in place.

1. Switch administered for 9600 Series IP Telephones.
2. LAN and applicable servers administered to accept the telephones.
3. Telephone software downloaded from the Avaya support site.
4. 46xxsettings file updated with site-specific information, as applicable.
5. 9600 Series IP Telephones installed. For more information, see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.
6. Individual 9600 Series IP Telephones updated using Craft procedures, as applicable. For more information, see “Local Administrative Procedures” in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

Administrative Checklist

Use the following checklist as a guide to system and LAN administrator responsibilities. This high-level list helps ensure that all telephone system prerequisites and requirements are met prior to telephone installation.

Note:

One person might function as both the system administrator and the LAN administrator in some environments.

Table 2: Administrative Checklist

Task	Description	For More Information See:
Network Requirements Assessment	Determine that network hardware is in place and can handle telephone system requirements.	Chapter 3: Network Requirements.
Administer the call server	Verify that the call server is licensed and is administered for Voice over IP (VoIP). Verify the individual telephones are administered as desired.	Chapter 4: Communication Manager Administration. Chapter 4: Communication Manager Administration.
DHCP server installation	Install a DHCP application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
Administer DHCP application	Add IP telephone administration to DHCP application.	DHCP Server Administration in Chapter 5: Server Administration.
HTTP/HTTPS server installation	Install an HTTP/HTTPS application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
Application file(s), script file, and settings file installation on HTTP/ HTTPS server	Download the files from the Avaya support site.	http://www.avaya.com/support Chapter 6: Telephone Software and Application Files.
Modify settings file as desired	Edit the settings file as desired, using your own tools.	Chapter 6: Telephone Software and Application Files.

1 of 2

Table 2: Administrative Checklist (continued)

Task	Description	For More Information See:
Administer WML servers	Add WML content as applicable to new or existing WML servers. Administer push content as applicable.	*Avaya one-X™Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-600888).
Administer telephones locally as applicable	As a Group:	The GROUP System Value on page 83 and the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide.*
	Individually:	The applicable Craft Local Procedures in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide.*
Installation of telephones in the network		*Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.
Allow user to modify Options, if applicable		OPSTAT on page 93 and the respective User Guide for the specific telephone model.

2 of 2

Telephone Initialization Process

These steps offer a high-level description of the information exchanged when the telephone initializes and registers. This description assumes that all equipment is properly administered ahead of time. This description can help you understand how the 9600 Series IP Telephones relate to the routers and servers in your network.

Step 1: Telephone to Network

The telephone is appropriately installed and powered. After a short initialization process, the telephone determines whether to carry out Virtual Private Network (VPN) procedures. If yes, the telephone establishes a VPN tunnel as appropriate for its administration. Once the VPN tunnel is established, or immediately after initialization for a non-VPN telephone, the telephone

identifies the LAN speed and sends a message out into the network, identifying itself and requesting further information. A router on the network receives and relays this message to the appropriate DHCP server.

Step 2: DHCP Server to Telephone

The DHCP file server provides information to the telephone, as described in DHCP and File Servers on page 55. Among other data passed to the telephone is the IP Address of the HTTP or HTTPS server.

Step 3: Telephone and File Server

The 9600 Series IP Telephones can download script files, application files, and settings files from either an HTTP or HTTPS server. The telephone queries the file server, which transmits a script file to the telephone. This script file, at a minimum, tells the telephone which application file the telephone must use. The application file is the software that has the telephony functionality.

The telephone uses the script file to determine if it has the proper application file. If the telephone determines the proper application file is missing, the telephone requests an application file download from the file server. The telephone then downloads the file and conducts some checks to ensure that the file was downloaded properly. If the telephone determines it already has the proper file, the telephone proceeds as described in the next paragraph without downloading the application file again.

The telephone checks and loads the application file, then uses the script file to look for a settings file, if appropriate. The optional settings file can contain settings you have administered for any or all of the 9600 Series IP Telephones in your network. For more information about this download process and settings file, see Chapter 6: Telephone Software and Application Files.

Step 4: Telephone and the Call Server

The call server referred to in this step is the Avaya Media Server.

In this step, the telephone might prompt the user for an extension and password. The telephone uses that information to exchange a series of messages with the call server. For a new installation and for full service, the user can enter the telephone extension and the password configured on the call server for that particular extension. For a restart of an existing installation, this information is already stored on the telephone, but the user might have to confirm the information. The telephone and the call server exchange more messaging. The expected result is that the telephone is appropriately registered and call server data such as feature button assignments are downloaded.

The 9600 Series IP Telephones support a feature called Unnamed Registration. Unnamed Registration allows a telephone to register with the call server without an extension, assuming the call server also supports this feature (i.e., unnamed registration is enabled through Avaya Communication Manager administration). To invoke Unnamed Registration, either enter a null (empty) extension or password or take no action. In the latter case, allow the **Extension...** prompt display for 60 seconds without making an entry. The telephone automatically attempts to register by means of Unnamed Registration. A telephone registered with Unnamed Registration has the following characteristics:

- only one call appearance,
- no administrable features,
- can make only outgoing calls, subject to call server Class of Restriction/Class of Service limitations, and
- can be converted to normal “named” registration by the user entering a valid extension and password.

You can also administer the telephone to avoid unnamed registration and remain unregistered if no extension and password are provided. For more information, see UNNAMEDSTAT in Table 11.

For more information about the installation process, see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

Error Conditions

Assuming proper administration, most of the problems reported by telephone users are likely to be LAN-based. Quality of Service, server administration, and other issues can impact user perception of IP telephone performance.

The *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide* covers possible operational problems that might be encountered after successful 9600 Series IP Telephone installation. The User Guides for a specific telephone model also contain guidance for users having problems with specific IP telephone applications.

Chapter 3: Network Requirements

Network Assessment

Perform a network assessment to ensure that the network will have the capacity for the expected data and voice traffic, and that it can support for all applications:

- H.323,
- DHCP,
- HTTP/HTTPS, and
- Jitter buffers.

Also, QoS support is required to run VoIP on your configuration. For more information, see Appendix B: Related Documentation and UDP Port Selection on page 39.

If you want any of your users to be able to use their 9600 Series IP Telephones to access your network through a Virtual Private Network (VPN), see the *VPN Setup Guide for 9600 Series IP Telephones* (Document 16-602968).

Hardware Requirements

To operate properly, you need:

- Category 5e cables designed to the IEEE 802.3af-2003 standard, for LAN powering,
- TN2602 or TN2302 IP Media Processor circuit pack. Sites with a TN2302 IP Media Processor circuit pack are strongly encouraged to install a TN2602 circuit pack to benefit from increased capacity.
- TN799C or D Control-LAN (C-LAN) circuit pack.

Important:

IP telephone firmware Release 1.0 or greater requires TN799C V3 or greater C-LAN circuit pack(s). For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya support Web site http://www.avaya.com/support.

To ensure that the appropriate circuit pack(s) are administered on your server, see Chapter 4: Communication Manager Administration. For more information about hardware requirements in general, see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

Server Requirements

Three server types can be configured for the 9600 Series IP Telephones:

- DHCP
- HTTP or HTTPS
- Web (optional)

While the servers listed provide different functions that relate to the 9600 Series IP Telephones, they are not necessarily different boxes. For example, DHCP provides file management whereas HTTP provides application management, yet both functions can co-exist on one hardware unit. Any standards-based server is recommended.

For parameters related to Avaya Server information, see Chapter 4: Communication Manager Administration, and the administration documentation for your call server. For parameters related to DHCP and file servers, see Chapter 5: Server Administration.

CAUTION:

The telephones obtain important information from the script files on the file server and depend on the application file for software upgrades. If the file server is unavailable when the telephones reset, the telephones operate based on their default administration and continue on to register with the call server. Some features might not be available. To restore them you need to reset the telephone(s) when the file server is available.

DHCP Server

Avaya recommends that a DHCP server and application be installed and that static addressing be avoided. Install the DHCP server and application as described in DHCP and File Servers on page 55.

HTTP/HTTPS Server

Administer the HTTP or HTTPS file server and application as described in HTTP Generic Setup on page 69.

Web Server (Optional)

If users have access to corporate WML Web sites, administer the telephones as described in Chapter 5: Server Administration.

For routine WML functionality only a WML server is required. For “push” functionality, a Trusted Push Server is needed. The Trusted Push Server can be the same server as your routine WML server. Separate the two functions for security purposes. Avaya recommends that you restrict access to push directories on the WML server.

Your Web server configuration must be compatible with the requirements covered in the *9600 Series IP Telephone Application Programmer Interface (API) Guide*.

Required Network Information

Before you administer DHCP and HTTP, and TLS, as applicable, complete the information in Table 3. If you have more than one Gateway, HTTP/TLS server, subnetwork mask, and Gatekeeper in your configuration, complete Table 3 for each DHCP server.

The 9600 Series IP Telephones support specifying a list of IP Addresses for a gateway/router, HTTP/HTTPS server, and Avaya Server gatekeeper(s). Each list can contain up to 255 total ASCII characters, with IP Addresses separated by commas with no intervening spaces. Depending on the specific DHCP application, only 127 characters might be supported.

When specifying IP Addresses for the file server or media server, use either dotted decimal format (“xxx.xxx.xxx.xxx”) or DNS names. If you use DNS, the system value DOMAIN is appended to the IP Addresses you specify. If DOMAIN is null, the DNS names must be fully qualified, in accordance with IETF RFCs 1034 and 1035. For more information about DNS, see DHCP Generic Setup on page 58 and DNS Addressing on page 103.

Table 3: Required Network Information Before Installation - Per DHCP Server

1. Gateway (router) IP Address(es)	
2. HTTP server IP Address(es)	
3. Subnetwork mask	
4. Avaya Server Gatekeeper IP Address(es)	
5. Avaya Media Server Gatekeeper port	Although this can be a value between 0 and 65535, the default value is **1719**. Do not change the default value unless that value conflicts with an existing port assignment.
6. HTTP/HTTPS server file path	
7. Telephone IP Address range *From*: *To*:	
8. DNS server address(es)	If applicable.
9. HTTPS server address(es)	If applicable.

The file server file path is the “root” directory used for all transfers by the server. All files are uploaded to or downloaded from this default directory. In configurations where the upgrade script and application files are in the default directory, do not use item 6 in Table 3.

As the LAN or System Administrator, you are also responsible for:

- Administering the DHCP server as described in Chapter 5: Server Administration.
- Editing the configuration file on the applicable HTTP or HTTPS file server, as covered in 9600 Series IP Telephone Scripts and Application Files.

Other Network Considerations

SNMP

The 9600 Series IP Telephones are fully compatible with SNMPv2c and with Structure of Management Information Version 2 (SMIv2). The telephones respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. “Fully compatible” means that the telephones respond to queries directed either at the MIB-II or the read-only Custom MIB. Read-only means that the values therein cannot be changed externally by means of network management tools.

You can restrict which IP Addresses the telephone accepts SNMP queries from. You can also customize your community string with system values SNMPADD and SNMPSTRING, respectively. 9600 Series IP Telephones support the functionality introduced with Avaya Communication Manager Release 4.0 that allows call server administration of the SNMP community string and SNMP Source IP Addresses. For more information, see Chapter 5: Server Administration and Table 11: 9600 Series IP Telephone Customizable System Parameters.

Note:

As of Release 1.1, SNMP is disabled by default. Administrators must initiate SNMP by setting the SNMPADD and SNMPSTRING system values appropriately.

For more information about SNMP and MIBs, see the IETF reference listed in Appendix B: Related Documentation. The Avaya Custom MIB for the 9600 Series IP Telephones is available for download in *.txt format on the Avaya support Web site at http://www.avaya.com/support.

Reliability and Performance

All 9600 Series IP Telephones respond to a ping or traceroute message sent from the call server switch or any other network source. The telephones do not originate a ping or traceroute. The 9600 Series IP Telephones offer and support “remote ping” and “remote traceroute.” The switch can instruct the telephone to originate a ping or a traceroute to a specified IP Address. The telephone carries out that instruction and sends a message to the switch indicating the results. For more information, see your switch administration documentation.

If applicable, the telephones test whether the network Ethernet switch port supports IEEE 802.1D/q tagged frames by ARPing the router with a tagged frame. For more information, see VLAN Considerations on page 100. If your LAN environment includes Virtual LANs (VLANs), your router must respond to ARPs for VLAN tagging to work properly.

For 9600 Series IP Telephones using a DHCP server, during DHCP processing the parameters listed in Table 8 are saved in the phone’s non-volatile memory so that the telephone can reuse the saved parameters if the DHCP server is not available for any reason during telephone restart or reboot.

QoS

For more information about the extent to which your network can support any or all of the QoS initiatives, see your LAN equipment documentation. See QoS on page 40 about QoS implications for the 9600 Series IP Telephones.

All 9600 Series IP Telephones provide some detail about network audio quality. For more information see Network Audio Quality Display on 9600 Series IP Telephones on page 28.

IEEE 802.1D and 802.1Q

For more information about IEEE 802.1D and IEEE 802.1Q and the 9600 Series IP Telephones, see IEEE 802.1D and 802.1Q on page 40 and VLAN Considerations on page 100. Three bits of the 802.1Q tag are reserved for identifying packet priority to allow any one of eight priorities to be assigned to a specific packet.

- **7:** Network management traffic
- **6:** Voice traffic with less than 10ms latency
- **5:** Voice traffic with less than 100ms latency
- **4:** “Controlled-load” traffic for critical data applications
- **3:** Traffic meriting “extra-effort” by the network for prompt delivery, for example, executive e-mail
- **2:** Reserved for future use
- **0:** The default priority for traffic meriting the “best-effort” for prompt delivery of the network

- **1:** Background traffic such as bulk data transfers and backups

  Note:

  Priority 0 is a higher priority than Priority 1.

Network Audio Quality Display on 9600 Series IP Telephones

All 9600 Series IP Telephones give the user an opportunity to monitor network audio performance while on a call. For more information, see the telephone user guide.

While on a call, the telephones display network audio quality parameters in real-time, as shown in Table 4.

Table 4: Parameters in Real-Time

Parameter	Possible Values
Received Audio Coding	***G.711***, ***G.722***, ***G.726A***, or ***G.729***.
Packet Loss	No data or a percentage. Late and out-of-sequence packets are counted as lost if they are discarded. Packets are not counted as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.
Packetization Delay	No data or an integer number of milliseconds. The number reflects the amount of delay in received audio packets, and includes any potential delay associated with the codec.
One-way Network Delay	No data or an integer number of milliseconds. The number is one-half the value RTCP or SRTCP computes for the round-trip delay.
Network Jitter Compensation Delay	No data or an integer number of milliseconds reporting the average delay introduced by the jitter buffer of the telephone.

The implication for LAN administration depends on the values the user reports and the specific nature of your LAN, like topology, loading, and QoS administration. This information gives the user an idea of how network conditions affect the audio quality of the current call. Avaya assumes you have more detailed tools available for LAN troubleshooting.

Qtest for Audio Quality

Qtest can be activated and the results displayed via the Avaya (A) Menu (or for the 9670, the Home screen), Phone Settings, Network Information option. When Qtest is activated, a UDP message containing a 4 octet Packet ID and a 4 octet Transmit Timestamp (with a precision of at least 1 millisecond) is sent every 20 milliseconds to the IP address specified by the value of QTESTRESPONDER. Each message is padded to a length of 180 octets (including the UDP header). A UDP port will only be opened for Qtest while it is active; see TCP/UDP Port Utilization on page 30 for the UDP port numbers applicable to Qtest.

The following values are generated from the echoed replies:

- the total number of packets sent,
- the total number of packets received,
- the percentage of packets lost,
- the largest number of sequential packets lost (the largest burst lost),
- the number of packets received out of sequence,
- the average round-trip delay,
- the maximum round-trip delay,
- the percentage of round trip delays longer than 400 milliseconds, and
- the average jitter (the number of milliseconds of delay introduced by the telephone's jitter buffer).

The end user can view the real-time values of these statistics when not on a call.

Note:

Some networks provide higher quality of service for RTP packets that use a specific UDP port range, so the same quality of service may not be applied to Qtest packets.

IP Address Lists and Station Number Portability

The 9600 Series IP Telephones provide the capability to specify IP Address lists. On startup or a reboot, the telephone attempts to establish communication with these various network elements in turn. The telephone starts with the first address on the respective list. If the communication is denied or times out, the telephone proceeds to the next address on the appropriate list and tries that one. The telephone does not report failure unless all the addresses on a given list fail, thereby improving the reliability of IP telephony.

This capability also has the advantage of making station number portability easier. Assume a situation where the company has multiple locations in London and New York, all sharing a corporate IP network. Users want to take their telephones from their offices in London and bring them to New York. When users start up their telephones in the new location, the local DHCP server usually routes them to the local call server. With proper administration of the local DHCP server, the telephone knows to try a second call server IP Address, this one in London. The user can then be automatically registered with the London call server.

Chapter 5: Server Administration contains details on administration of DHCP servers for lists of alternate media servers, router/gateways, and HTTP/HTTPS servers. For more information, see DNS Addressing on page 103.

TCP/UDP Port Utilization

The 9600 Series IP Telephones use a variety of protocols, particularly TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and TLS (Transport Layer Security) to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP ports each piece of equipment uses to support each protocol and each task within the protocol. For additional TCP/UDP port utilization information as it applies to Avaya Communication Manager, see UDP Port Selection on page 41.

Depending on your network, you might need to know what ports or ranges are used in the operation of 9600 Series IP Telephones. Knowing these ports or ranges helps you administer your networking infrastructure.

Note:

In many cases, the ports used are the ones called for by IETF or other standards bodies.
Some of the explanations in Table 5 and Table 6 refer to configuration parameters or options settings. For more information about parameters and settings, see Administering Options for the 9600 Series SIP IP Telephones.

Table 5: Received Packets (Destination = 9600 Series IP Telephone)

Destination Port	Source Port	Use	UDP or TCP?
The number used in the Source Port field of Qtest packets sent by the phone	7	Received Qtest messages	UDP
The number used in the Source Port field of DNS packets sent by the telephone	Any	Received DNS messages	UDP
The number used in the Source Port field of the packets sent by the telephone's HTTP client	Any	Packets received by the telephone's HTTP client	TCP
Release 2.0+ = PUSHPORT Pre-Release 2.0 = 80	Any	Packets received by the telephone's HTTP server	TCP
500, 2070, or 4500	500 or 4500	Received IKE or IPsec messages (if NVIKEOVERTCP is 1 or 2)	TCP
The number used in the Source Port field of the TLS/ SSL packets sent by the telephone's HTTP client	Any	TLS/SSL packets received by the telephone's HTTP client	TCP
68	Any	Received DHCP messages	UDP
161	Any	Received SNMP messages	UDP

1 of 2

Table 5: Received Packets (Destination = 9600 Series IP Telephone) (continued)

Destination Port	Source Port	Use	UDP or TCP?
500, 2070, or 4500	500 or 4500	Received IKE or IPsec messages (if NVIKEOVERTCP is 0 or 1)	UDP
50000	Any	Received CNA (Chatter) test request messages	UDP
The number used in the Source Port field of registration messages sent by the telephone's CNA test plug	Any	Received CNA (Chatter) registration messages	TCP
PORTAUD or the port number reserved for CNA RTP tests	Any	Received RTP and SRTP packets	UDP
PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd) or the port number reserved for CNA RTP tests plus or minus one, as for PORTAUD, above	Any	Received RTCP and SRTCP packets	UDP
System-Specific	Any	Received signaling protocol packets	UDP/TCP

2 of 2

Table 6: Transmitted Packets (Source = 9600 Series IP Telephone)

Destination Port	Source Port	Use	UDP or TCP?
7	Any unused port number	Transmitted Qtest messages	UDP
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
Release 2.0+ = HTTPPORT Pre-Release 2.0 = 80 unless explicitly specified otherwise (i.e. use of Port 81 for CM)	Any unused port number	Packets transmitted by the telephone's HTTP client during startup	TCP
80 unless explicitly specified otherwise (e.g., in a URL or due to use of WMLPORT)	Any unused port number	Packets transmitted by the telephone's HTTP client after startup (for example, for backup/restore or push)	TCP

1 of 3

Table 6: Transmitted Packets (Source = 9600 Series IP Telephone) (continued)

Destination Port	Source Port	Use	UDP or TCP?
The number used in the Source Port field of the SNMP query packet received by the telephone	161	Transmitted SNMP messages	UDP
The number used in the Source Port field of packets received by the telephone's HTTP server	Release 2.0+ = PUSHPORT Pre-Release 2.0 = 80	Packets transmitted by the telephone's HTTP server	TCP
Release 2.0+ = TLSPORT Pre-Release 2.0 = 411	Any unused port number	TLS/SSL packets transmitted by the telephone's HTTP client during startup	TCP
443 unless explicitly specified otherwise (i.e. in a URL)	Any unused port number	TLS/SSL packets transmitted by the telephone's HTTP client after startup (for example, for backup/restore)	TCP
500 or 4500	500, 2070, or 4500	Transmitted IKE or IPsec messages (if NVIKEOVERTCP is 0 or 1)	TCP
514	Any unused port number	Transmitted Syslog messages	UDP
33434 - 33523 (starts with 33434, increments by 1 for each message sent, 3 messages per hop, up to 30 hops)	Any unused port number	Transmitted traceroute messages	UDP
CNAPORT	Any unused port number	Transmitted CNA (Chatter) registration messages	TCP
The port number specified in the test request message	50000	Transmitted CNA (Chatter) test results messages	UDP
System-specific	system - specific	Transmitted signaling protocol packets	TCP
FEPORT or the port number specified in a CNA RTP test request	PORTAUD, or the port number reserved for CNA RTP tests	Transmitted RTP and SRTP packets	UDP

2 of 3

Table 6: Transmitted Packets (Source = 9600 Series IP Telephone) (continued)

Destination Port	Source Port	Use	UDP or TCP?
FEPORT + 1 (if FEPORT is even) or FEPORT -1 (if FEPORT is odd) or the port number specified in a CNA RTP test request plus or minus one, as with FEPORT above	PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd) or the port number reserved for CNA RTP tests plus or minus one, as for PORTAUD, above	RTCP and SRTCP packets transmitted to the far-end of the audio connection	UDP
RTCPMONPORT	PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd)	RTCP packets transmitted to an RTCP monitor	UDP
System-specific	System - specific	Transmitted signaling protocol packets	UDP

Security

For information about toll fraud, see the respective call server documents on the Avaya support Web site. The 9600 Series IP Telephones cannot guarantee resistance to all Denial of Service attacks. However, there are checks and protections to resist such attacks while maintaining appropriate service to legitimate users.

All 9600 Series IP Telephones that have WML Web applications support Transport Layer Security (TLS). This standard allows the telephone to establish a secure connection to a HTTPS server, in which the upgrade and settings file can reside. This setup adds security over another alternative.

You also have a variety of optional capabilities to restrict or remove how crucial network information is displayed or used. These capabilities are covered in more detail in Chapter 5: Server Administration.

- Support signaling channel encryption while registering, and when registered, with appropriately administered Avaya Media Servers.

  Note:

  Signaling and audio are not encrypted when unnamed registration is effective.

- Restricting the response of the 9600 Series IP Telephones to SNMP queries to only IP Addresses on a list you specify.
- Specifying an SNMP community string for all SNMP messages the telephone sends.
- Restricting dialpad access to Local Administration Procedures, such as specifying IP Addresses, with a password.
- Restricting dialpad access to Craft Local Procedures to experienced installers and technicians.
- Restricting the end user's ability to use a telephone Options application to view network data.
- As of Release 2.0, 9600 Series IP Telephones can download and use third-party trusted certificates.
- As of Release 1.5, 9600 Series IP Telephones are fully compliant with IETF RFC 1948 *Defending Against Sequence Number Attacks*, May 1996, by S. Bellovin.
- As of Release 1.5, three existing security-related parameters can be administered on the call server and downloaded with encrypted signaling, in addition to unencrypted HTTP or encrypted HTTPS. Those parameters are SNMP community string, SNMP Source IP Addresses, and Craft Access Code (PROCPSWD).

Registration and Authentication

Avaya call servers support using the extension and password to register and authenticate 9600 Series IP Telephones. For more information, see the current version of your call server administration manual.

Time-to-Service (TTS)

The IP Endpoint Time-to-Service (TTS) feature was introduced in Software Release 1.2.1, along with Avaya Communication Manager (CM) Release 4.0. TTS changes the way IP endpoints register with their gatekeeper, reducing the time to come into service. Without TTS, IP endpoints are brought into service in two steps, which are coupled: (1) H.323 registration and (2) TCP socket establishment for call signaling. The TTS feature de-couples these steps. In CM 4.0, IP endpoints can be enabled for service with just the registration step. TCP sockets are established later, as needed.

The TTS feature also changes the direction of socket establishment. With TTS, Communication Manager, rather than the endpoint, initiates socket establishment, which further improves

performance. In CM 4.0, TTS is enabled by default, but can be disabled for all IP endpoints in a given IP network region by changing the IP Network form. TTS applies only to IP endpoints whose firmware has been updated to support this feature. It does not apply to the following endpoints: third party H.323, DCP, BRI, and analog.

As of software Release 3.0, 9600 Series IP Telephones will accept an incoming connection request from a server on their gatekeeper list, use this new connection to replace an existing connection, and continue operation without the need to re-register. This mechanism allows CM to quickly originate a new connection to each of these telephones during a server interchange, causing the telephones to move quickly to the server and transitioning from the standby to active state.

For more information, see the *Administrator Guide for Avaya Communications Manager* (Document Number 03-300509).

Chapter 4: Communication Manager Administration

Call Server Requirements

Before you perform administration tasks, ensure that the proper hardware is in place, and your call server software is compatible with the 9600 Series IP Telephones. Avaya recommends the latest PBX software and the latest IP telephone firmware.

Switch Compatibility and Aliasing IP Telephones

As of Release 1.2, 9600 Series IP Telephones were natively supported by Avaya Communication Manager (CM) Release 4.0. Native support means that if you have CM 4.0 or greater, you:

- do not have to alias 9600 Series IP Telephones, with the exception of the 9670G, which is not natively supported and must be aliased as a 9630.
- can add up to three SBM24 Button Modules on each 9600 Series IP Telephone that supports an SBM24, and
- can administer a call coverage telephone number on a station-by-station basis.

If you have Avaya Communication Manager (CM) Release 3.1 you must alias the telephones as follows:

9600 Series Telephone Model	Aliased as...	Earliest CM Release
9610	4610SW	CM 3.1
9620/9620L/9620C	4610SW (recommended)	CM 3.1
	4620SW	CM 3.1
9630/9630G	4620SW	CM 3.1
9640/9640G	4620SW	CM 3.1
9650/9650C	4620SW	CM 3.1
9670G	4620SW 9640	CM 3.1 CM 4.0

Note:

Although the 9620/9620L/9620C can be aliased as a 4620SW IP Telephone, some features are not available. For example, the 9620 phones only support a total of 12 call appearances and administered feature buttons. The 4620 can be administered for a total of 24 call appearances and feature buttons.

For specific administration instructions about aliasing 9600 Series IP Telephones, see Administering Stations on page 46.

When a 9610 IP Telephone is aliased as a 4610SW IP Telephone, its four administrable call appearances/features should be:

- one primary call appearance
- the Directory, Next, and Make Call feature buttons (hard-coded with CM 4.0 or later)

The 9610 ignores any other features or call appearances.

When a 9620/9620L/9620C IP Telephone is aliased as a 4620SW IP Telephone, do not administer:

- a button module (SBM24, EU24, or EU24BL), or
- feature buttons 13 through 24.

The 9630/9630G, 9640/9640G, 9650/9650C, and 9670G IP Telephones support twenty-four administrable telephony call appearances or features. In addition, the 9630/9630G, 9640/9640G, 9650/9650C, and 9670G IP Telephones support the SBM24 Button Module. These models always support a single SBM24, and within CM 4.0 or later, support up to three SBM24 Button Modules per telephone.

The SBM 24 Button Module provides another twenty-four administrable call appearances and features. The button module can be used freestanding or attached directly to the 9630/9630G, 9640/9640G, 9650/9650C, or 9670G.

Call Server (Switch) Administration

For switch administration information not covered in this chapter, see the following documents on the Avaya support Web site:

- The *Administrator Guide for Avaya Communication Manager* (Document Number 03-300509) provides detailed instructions for administering an IP telephone system on Avaya Communication Manager. See Chapter 3 “Managing Telephones,” which describes the process of adding new telephones. Also, you can locate pertinent screen illustrations and field descriptions in Chapter 19 “Screen References” of that guide.
- *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504) provides detailed information about switch administration for your network.

IP Interface and Addresses

Follow these general guidelines:

- Define the IP interfaces for each CLAN and Media processor circuit pack on the switch that uses the IP Interfaces screen. For more information, see *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504).
- On the Customer Options form, verify that the **IP Stations** field is set to "**y**" (Yes). If it is not, contact your Avaya sales representative. The **IP Softphone** field does not have to be set to "**y**" (Yes).

UDP Port Selection

The 9600 Series IP Telephones can be administered from the Avaya Communication Manager Network Region form to support UDP port selection. Locate specific port assignment diagrams in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*. For information about Avaya Communication Manager implementation, see *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504) on the Avaya support Web site.

Administer the switch to use a port within the proper range for the specific LAN, and the IP telephone(s) copy that port. If no UDP port range is administered on the switch, the IP telephone uses an even-numbered port, randomly selected from the interval 4000 to 10000.

RSVP and RTCP/SRTCP

Avaya IP Telephones implement the Resource ReSerVation Protocol (RSVP) and the RTP/SRTP Control Protocol (RTCP/SRTCP). RTCP Monitor Server software can then provide real-time monitoring and historical data of audio quality for VoIP calls.

Note:

Only the counter mode of the AES-128 encryption algorithm is supported. Encryption of SRTCP is not supported.

The only way to change these parameters is by appropriate switch administration. For more information, see your Avaya server administration documentation and *Administration for Network Connectivity for Avaya Communication Manager (*Document Number 555-233-504).

QoS

The 9600 Series IP Telephones support both IEEE 802.1D/Q and DiffServ. Other network-based QoS initiatives such as UDP port selection do not require support by the telephones. However, they contribute to improved QoS for the entire network.

IEEE 802.1D and 802.1Q

The 9600 Series IP Telephones can simultaneously support receipt of packets using, or not using, 802.1Q parameters. To support IEEE 802.1D/Q, you can administer 9600 Series IP Telephones from the network by appropriate administration of the DHCP or HTTP/HTTPS servers, or by using dialpad input at the telephone.

Important:

Avaya Communication Manager administration always takes precedence over manual administration of IEEE 802.1D/Q data.

The four IEEE 802.ID/Q QoS parameters in the telephones that can be administered on the IP Network Region form are **L2Q, L2QVLAN, L2QAUD, and L2QSIG.** To set these parameters at the switch, see “About Quality of Service (QoS) and voice quality administration” in *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504). To set these parameters manually see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide.* You can specify VLAN ID and VLANTEST values with the ADDR Local Administrative Option.

Note:

All Craft local procedures are on a phone-by-phone basis. Administration using Communication Manager, DHCP, and HTTP applies to the telephone system itself or to a range of telephones.

NAT

Network Address Translation (NAT) usage can lead to problems that affect the consistency of addressing throughout your network. All H.323 IP Telephones support NAT interworking. Support for NAT does not imply support for Network Address Port Translation (NAPT). The telephones do not support communication to the PBX through any NAPT device.

NAT requires specific administration on the media server. A direct Avaya IP Telephone-to-Avaya IP Telephone call with NAT requires Avaya Communication Manager Release 3.0 or greater software. For more information, see *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504) on the Avaya support Web site.

DIFFSERV

The DiffServ values change to the values administered on the call server as soon as the telephone registers. For more information, see Chapter 4 “Network Quality Administration” in *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504). Unless there is a specific need in your enterprise LAN, Avaya recommends that you do not change the default values.

Voice Mail Integration

9600 Series IP Telephones with CM 4.0+ Native Support

Release 1.2 provides native support for 9600 Series IP Telephones running on Avaya Communication Manager (CM) Release 4.0 or later. When native support applies, pressing the **Messages** button causes the telephone to first determine if the call server has a dedicated number for retrieving voice mail and when found, to proceed with voice mail retrieval.

9600 Series IP Telephones Aliased as 4600 Series IP Telephones

When native support does not apply, 9600 Series IP Telephones are aliased as 4600 Series IP Telephones and run under a CM Release earlier than 4.0. In this case, use the settings file to configure the **Messages** button by setting the system parameter MSGNUM to any dialable string. MSGNUM examples are:

- a standard telephone number the telephone should dial to access your voice mail system, such as AUDIX or Octel.
- a Feature Access Code (FAC) that allows users to transfer an active call directly to voice mail. FACs are supported only for QSIG-integrated voice mail systems like AUDIX or Octel. QSIG is an enhanced signaling system that allows the voice mail system and Avaya Communication Manager Automated Call Processing (ACP) to exchange information.

When the user presses the **Messages** button on the telephone, that number or FAC is automatically dialed, giving the user one-touch access to voice mail.

The settings file specifies the telephone number to be dialed automatically when the user presses this button. The command is:

SET MSGNUM *1234*

where ***1234*** is the Voice Mail extension (CM hunt group or VDN). For more information, see Table 11.

Note:

MSGNUM is only used when the telephone is aliased using non-native support. Messaging must be configured for native support.

A separate Voice Mail extension can be administered for each station.

Call Transfer Considerations

This section provides information about call transfer behaviors to consider when administering the call server. The telephone application presents a user interface, based in part on the deduction of the call state. But, as the administrator, be aware that the following server-based features can interact with the user interface resulting in a call state that might need explanation:

- When the system parameter **Abort Transfer?** is set to *Yes*, once a transfer has been started the user cannot press a non-idle call appearance until the transfer is complete or the transfer is aborted.
- When the system parameter **Abort Transfer?** is set to *No*, the transfer proceeds normally even if the user presses a non-idle call appearance before the transfer is complete.
- When the system parameter **Transfer Upon Hang-up** is set to *No*, the user must press the **Complete** softkey after dialing the intended destination for the transfer to be completed.
- When the **Transfer Upon Hang-up** is set to *Yes*, the user can hang up immediately after dialing and the transfer proceeds normally.

The features **Abort Transfer** and **Transfer Upon Hang-up** can interact. If a user initiates a transfer, dials the destination, and hangs up without pressing the **Complete** softkey, the three possible outcomes are:

- The transfer is completed. This is the case when **Transfer Upon Hang-up** is set to *Yes*, regardless of the **Abort Transfer?** setting.
- The transfer is aborted. This is the case when **Transfer Upon Hang-up** is set to *No* and **Abort Transfer?** is set to *Yes*.
- The transfer is denied. This is the case when **Transfer Upon Hang-up** is set to *No* and **Abort Transfer?** is set to *No* and the call appearance of the transferee remains on soft hold.

Attempts to transfer an outside call to an outside line are denied. However, the user can drop the denied destination and initiate a transfer to an internal destination.

The call server feature, **Toggle Swap**, allows the user to swap the soft-held and setup call appearances. That is, the setup call appearance becomes soft-held, and the soft-held call

appearance becomes active as the setup call appearance. This only works once the setup call appearance is connected on a call. If Toggle Swap is pressed while the setup call appearance has ringback, the call server sends a broken flutter to the setup call appearance. Toggle Swap is ignored without a broken flutter if pressed while the setup call appearance is still dialing. Toggle swapping the hold status of call appearances can be confusing to the user.

Conferencing Call Considerations

This section provides information about conference call behaviors to consider when administering the call server. The telephone application presents a user interface, based in part on the deduction of the call state. But, as the administrator, be aware that the following server-based features can interact with the user interface resulting in a call state that might need explanation:

- When the system parameter **Abort Conference Upon Hang-up** is set to *Yes*, the user must dial and press the **Complete** softkey for the conference to be completed. If the user hangs up during conference setup before pressing **Complete**, the conference is cancelled with the held party remaining on [hard] hold. When the system parameter **Abort Conference Upon Hang-up** is set to *No*, the user can hang up immediately after dialing, dial a third party, then press the **Complete** softkey to have the conference proceed normally.
- When the system parameter **No Dial Tone Conferencing** is set to *No*, and the **Conference** or **Add** softkey is pressed, the call server automatically selects an idle call appearance for the user to dial on. This action allows the next conferee to be added. When the system parameter **No Dial Tone Conferencing** is set to *Yes*, the user must manually select a call appearance after pressing the **Conference** or **Add** softkey.

Conferencing behavior changes significantly when **Select Line Conferencing** is set to *Yes*, which automatically sets **No Dial Tone Conferencing** to *Yes*. Specifically:

- If the user finishes dialing the intended conferee, pressing the initial call appearance completes the conference, as if the **Join** softkey was pressed.
- If the user has not finished dialing the intended conferee, pressing the initial call appearance (placed on soft hold when **Conference** or **Add** was pressed) cancels the conference set up.
- If the user presses the **Conference** or **Add** softkey, then immediately presses a hard-held call appearance, the previously held call appearance is retrieved from hold and joins the existing conference.

When the system parameter **Select Line Conferencing** is set to *No*, the user cancels the conference setup by pressing the call appearance on soft hold before pressing **Join**. Selecting a hard-held call appearance during conference setup establishes the held call as the intended conferee.

For either Select Line Conferencing setting, if the user is in conference setup and answers an incoming call, the incoming call is established as the intended conferee; the user must press

Join to add the answered call to the conference. If the user does not want the incoming call to be part of the conference, the call should not be answered, or the call can be answered and then hung up before continuing the conference setup. Pressing an in-use call appearance during conference setup makes that call appearance the intended conferee. The **Toggle Swap** feature works for Conference setup just like it does for Transfer Setup. For more information, see the last paragraph of Call Transfer Considerations.

Telephone Administration

System-Wide Administration

This section refers to Communication Manager (CM) administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. The system wide CM form and the particular page that needs to be administered for each feature are provided. These features, which already exist, are not required but are recommended because they optimize the telephone user interface. CM 3.0 or greater is required.

Note:

See Appendix C: Sample Administration Forms for illustrated examples of the pages used to administer Communication Manager features.

Feature-Related System Parameters

Release 1.5 supports the functionality introduced on Avaya Communication Manager Release 4.0 that allows call server administration of three system-wide parameters. By administering these parameters on CM, they can be automatically downloaded to the telephone during registration, instead of or in addition to from the settings file or locally per telephone. The three system parameters are: SNMP community string, SNMP Source IP addresses, and Craft Access Code (PROCPSWD). Administer these three parameters using Page 3 of the change system-parameters ip-options form.

Communication Manager Feature Administration

Feature	Administration
On-Hook Dialing	Set up CM so that the phone supports on-hook dialing. Use the System Parameters Features form page 10. Use the command **`Change system-parameters features`** to view the form and make the change.

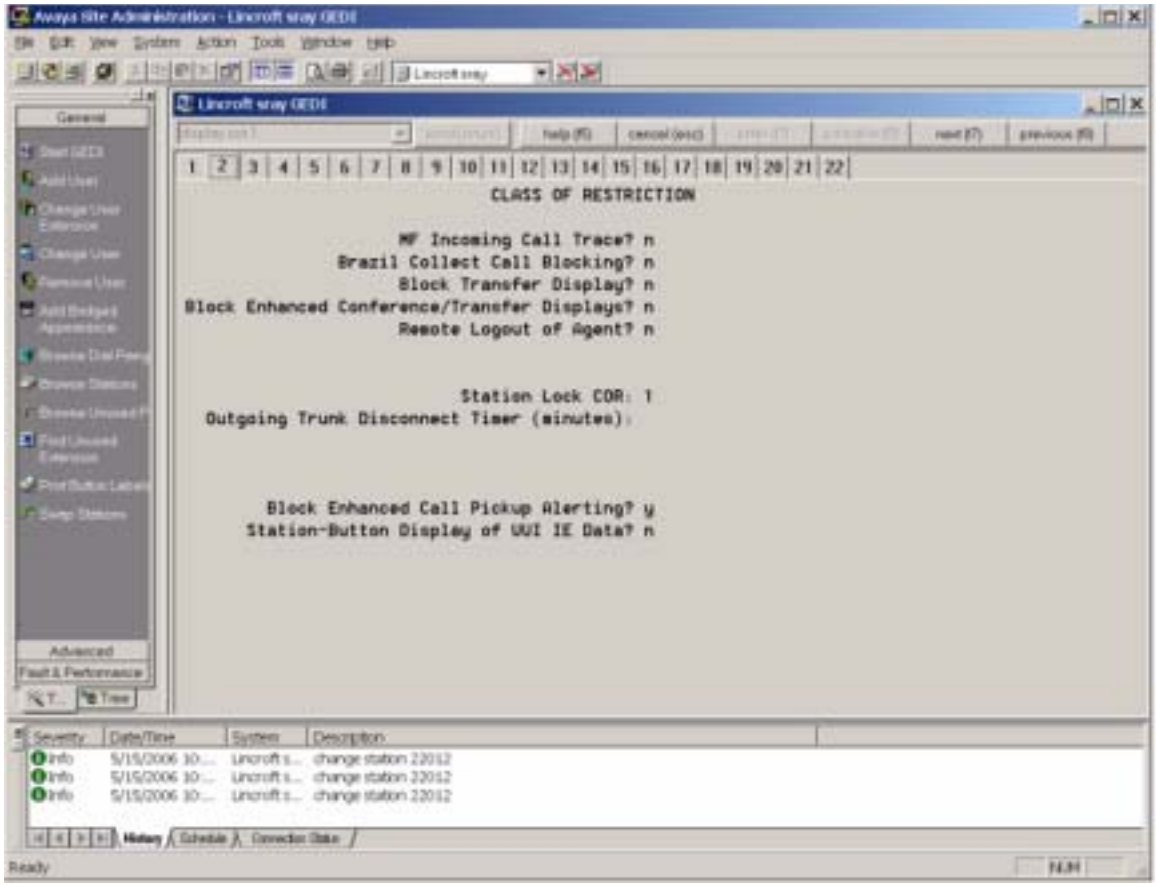
1 of 2

Communication Manager Feature Administration (continued)

Feature	Administration
Auto Hold	Set up CM to enable **Auto Hold**, so that the phone automatically places an active call on hold when the user answers or resumes a call on another call appearance. Use the System Parameters Features form, page 6.
Coverage Path	Administer a coverage path for both phone demonstration and normal operations. Use the Coverage Path form and give it a number, for example, Coverage path 1. If Voice Mail is available, this is also where you administer the hunt group or VDN, depending on the type of VM system being used.
Enhanced Conference Features	Enable enhanced conference display to support the user experience for conferences. Block Enhanced Conference Display on the Class of Restriction (COR) form must be set to **No**. Use the command **`Change COR`**, followed by a number, to view the form and make the change. a sample of the Class of Restriction form.
EC500	If EC500 licenses have been acquired, enable EC500 on the Off-PBX Telephones Station Mapping form. This feature requires trunking to work properly. Use the following command to make the change: **`Change Off-pbx Telephone Mapping`**
Wideband Audio	To enable Wideband Audio, use the **`Change IP codec`**: command on CM. Ensure that **G.722-64K** is first on the list of codecs. Note that wide band audio works only for direct-IP calls between two 96xx endpoints, either with both registered to the same server, or registered to different servers when connected by IP trunks. Calls between two 96xx phones connected by an IP trunk do not currently support wide band audio when the call is shuffled such that the media travels directly between the two 96xx IP telephones. Calls involving three or more parties, even if they are all 96xx IP telephones, will not use wide band. Calls between two 96xx IP telephones where audio is terminated at a port network/gateway (PN/GW) media resource will not use wideband. Ensure that G.722 is added to all codec-sets that can possibly be used between all regions on the IP-Network Regions form where 96xx IP telephones exist. Technically, G722 does not need to be first. What is needed, however, is that all the non media processor-supported codecs (G722, SIREN, etc.) be placed before the media processor-supported codecs (G711, G729, G726, G723).

2 of 2

Figure 1: Sample Class of Restriction (COR) Form


CLASS OF RESTRICTION
MF Incoming Call Trace? n
Brazil Collect Call Blocking? n
Block Transfer Display? n
Block Enhanced Conference/Transfer Displays? n
Remote Logout of Agent? n
Station Lock COR: 1
Outgoing Trunk Disconnect Timer (minutes):
Block Enhanced Call Pickup Alerting? y
Station-Button Display of UUI IE Data? n

Administering Stations

This section refers to Communication Manager (CM) administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. Administer the following items on the Station form, sample screens of which are provided in Figure 6 through Figure 9. Avaya recommends setting the features covered in this section because they optimize the user interface.

Release 1.5 supports the functionality introduced on Avaya Communication Manager Release 4.0 that allows call server administration of the GROUP parameter on a station-by-station basis. As covered in The GROUP System Value on page 83, the GROUP Identifier can be used in conjunction with the 46xxsettings file to allow administration to apply to specific “groups” of telephones. Before Release 1.5, the Group Identifier had to be administered locally on each applicable telephone. As of Release 1.5, the Group Identifier can be administered centrally, and downloaded to each applicable telephone. The GROUP ID parameter is administered on page 3 of the Change Station Form. Once downloaded, the Group Identifier takes effect starting with the next telephone boot-up.

For sample Station Forms, see Appendix C: Sample Administration Forms.

Aliasing 9600 Series IP Telephones

Communication Manager releases earlier than 4.0 do not provide native support for 96xx IP Telephones. On the Station Form, administer (alias) the telephones as follows:

Change Alias Station:

- Alias set up type 9610 to a 4610
- Alias set up type 9620 to a 4610
- Alias set up type 9630/9630G to a 4620SW/4621SW
- Alias set up type 9640/9640G to a 4620SW/4621SW
- Alias set up type 9650 to a 4620SW/4621SW
- Alias set up type 9670G to a 4620SW/4621SW

Communication Manager release 4.0 (and later) provides native support for the 9610, 9620, 9630/9630G, 9640/9640G, and 9650. With CM 4.0 (and later), the 9670G must be aliased as a 9630 IP Telephone. Softphone is currently not supported using native support of the 96xx phones.

Note:

Call appearances are not configurable for native support of the 9610 in CM 4.0. Care should be taken when aliasing the 9610 as a 4610, since the call appearances are configurable but must adhere to the unique 9610 administrative guidelines found in For the 9610 IP Telephone on page 48 and Special Administration for the 9610 IP Telephone.

Administering Features

The following are administrable Station Features that Avaya recommends you administer for your 9600 Series IP Telephones for maximum user experience.

Administrable Station Features

Feature	Administration
Enhanced Conference Features	Administer **Conf-dsp** (conference display) on the station form as a feature button. Doing so turns on enhanced conference features and gives users advanced conference features.
Far End Mute	Administer **fe-mute** (far end mute). When this is enabled the phone shows a “Silence” softkey on the Conference details screen. This feature works only for trunk calls.
Send All Calls (SAC)	On the Station form, administer **SAC** (send-calls) as a feature button. On the Station form to the right of where send all calls is administered, leave the extension box empty. This feature requires a coverage path to be administered on the station form.

1 of 2

Administrable Station Features (continued)

Feature	Administration
Coverage Path	For normal operation, you must set up a coverage path for each telephone. Administer the Station form to point to the appropriate system coverage path, for example, coverage path 1.
Auto select any idle appearance	Set **Auto select any idle appearance** to **N** (no) to optimize answering calls.
Restrict Last Call Appearance	Set **Restrict Last Call Appearance** to **Y** (yes).
Conference/Transfer on Primary Appearance	Set **Conference/Transfer on Primary Appearance** to **Y** (yes) to ensure that conference/transfer of a bridged appearance works properly.

2 of 2

Feature Buttons and Call Appearances

For the 9610 IP Telephone

The 9610 must be administered on releases earlier than CM3.1 as a 4610. On Release CM4.0 and later, administer the 9610 as a 9610. The 9610 has only one line appearance. As a consequence, you must follow these CM administration steps:

- Administer the first call appearance/feature button on the CM Station form as a call appearance.
- Administer “Directory,” "Next," and “Call-disp (the latter being shown as "Make Call" on the telephone) as the next three feature buttons. This is hard-coded on CM 4.0.
- Anything administered beyond the first six call appearances will be ignored. On CM4.0 the call appearance/feature button assignments are hard- coded.

Important:

Set “Restrict last appearance” to “n” (no) on the Station form so that incoming calls can be placed and outgoing calls can be answered.

Note:

A 9610 IP telephone does not reflect CM administrative changes until the telephone is reset/restarted. The 9610 does not support the SBM24 button module.

For the 9620/9620L/9620C IP Telephone

You can administer Feature/Call Appearance Buttons 1 – 12 on the CM Station form, which the telephone Feature screen then displays in sequence. The telephone does not display any of the Feature Button labels administered on buttons 13 – 24. The 9620 does not support the SBM24 Button Module.

For 9630/9630G, 9640/9640G, 9650/9650C, and 9670G IP Telephones

You can administer Feature/Call Appearance Buttons 1 – 24 on the CM Station form. The features administered on the Station form appear in the same sequence on the telephone Feature screen. Features administered on the Expansion Module SBM24 Call Appearance buttons display on the telephone Features screen following the first 24 administered feature buttons. All administered SBM24 Button Labels (Call Appearances and Feature Buttons) display on the corresponding SBM24 module buttons.

In Table 7 the term “phone screen” refers to either the call appearance screen or the features screen, as applicable to the button type.

Table 7: Station Form Administration Results

Feature / Call Appearance (CA) / Bridged Call Appearance (BA) buttons on the Station form...	Is displayed on the phone as:			
	9620/9620L/ 9620C	**9630/9630G 9640/9640G**	**9650/9650C**	**9670G**
1 to 3	Phone screen	Phone screen	Phone screen	Phone screen

1 of 2

Table 7: Station Form Administration Results (continued)

Feature / Call Appearance (CA) / Bridged Call Appearance (BA) buttons on the Station form...	Is displayed on the phone as:			
	9620/9620L/ 9620C	**9630/9630G 9640/9640G**	**9650/9650C**	**9670G**
4 to 11	CAs/BAs on Phone screen; must scroll to see more than 3	CAs/BAs on Phone screen: must scroll to see more than 6	Aux buttons 1 to 8 CAs/BAs on Phone screen; must scroll to see more than 3	CAs/BAs on Phone screen; all buttons also appear on the Quick Touch panel (if enabled) and not on the display screen. If Quick Touch panel is disabled, 6 CAs display; switch to Features and scroll to see up to 12 feature buttons
12 to 19	N/A	Scroll to see CAs/BAs, features on Feature List	Aux buttons 9 to 16	Scroll to see CAs/BAs, features on Feature List
20 to 24	N/A	Features on Feature List	Features on Feature List	Features on Feature List
25 to 48	N/A	1st SBM24	1st SBM24	1st SBM24
49 to 72	N/A	2nd SBM24	2nd SBM24	2nd SBM24
73 to 96	N/A	3rd SBM24	3rd SBM24	3rd SBM24

2 of 2

For additional information about administering the call server for 9600 Series IP Telephones, see the following Avaya documents, available on the Avaya Support Web site:

- *Administrator Guide for Avaya Communication Manager* (Document Number 03-300509).
- *Feature Description and Implementation for Avaya Communication Manager* (Document Number 555-245-770).

Enhanced Phone Screen Display for 9630/9630G and 9640/9640G IP Telephones

For the 9630/9630G/9640/9640G telephones, if the system parameter FBONCASCREEN has value "1" the telephone determines the total number of call appearances (primary or bridged) that have been administered for the telephone (plus any adjunct button modules, if applicable).

If the total number of call appearances is less than six, then all call appearances (primary or bridged) that have been administered for the telephone (including any adjunct button modules, if applicable) are displayed in order. The remaining Application Lines display the first administered feature buttons for the telephone, in order from top to bottom without any gaps. Note that this applies to administered feature buttons for the telephone only; administered feature buttons for any adjunct button module are not displayed on this list.

9650/9650C Aux Button Assignments

The 9650/9650C CM 4.0 Station form assigns buttons 4 to 11 to the Aux Labels 1 to 8, and buttons 12 to 19 to the shifted view of Aux buttons 9 to 16. CM button assignments 20-24 do not appear on the Aux button labels. Additionally, any call appearances that are assigned to CM buttons 4 through 24, like all the 96xx phones, appear on the Phone screen in a scrollable list. Any feature assigned to CM buttons 4 through 24, like the other 96xx phones, appears on the features list (reached by pressing the left or right arrow key while viewing the call appearances screen on the phone).

Button Module(s) (SBM24) on the 9630/9630G, 9640/9640G, 9650/9650C, and 9670G

Use the 9630/9630G, 9640/9640G, or 9650/9650C Station form to enable the SBM24 Button (Expansion) Module(s) and administer Call Appearances as primary appearances, bridged appearances, or busy indicators.

If the SBM24 Call Appearance corresponding to the CM call-associated display message or dialed-digits string is not visible because the user is not on the Phone screen, the telephone Top Line displays the call-associated display message or dialed-digits string.

Conference Details Screen for Ad-Hoc Conferences

Conference Details allows the user to view parties on a conference call and selectively mute or drop individual parties for a conference call setup.

If administered on an Expansion Module button, the SBM24 Button Module must be connected.

To enable Conference Details capabilities:

1. On the Class of Restriction (COR) form make sure that **Block Enhanced Conference/ Transfer Displays** is set to **No**.
2. As described in On-Hook Dialing, administer the Conference Display Feature Button to a Phone button on the Phone screen.

Special Considerations for the 9650/9650C IP Telephone

Call appearances, bridged call appearances, or features can be displayed on the 16 Aux button labels. The telephone displays eight labels at a time on the bottom two rows of the screen. Users can toggle between the two sets of 8 labels using the Aux shift button to the right of the Aux labels.

- The Aux button label area can fit 6-7 characters, depending on the width of the characters used.
- Cluster any call appearances together, bridged call appearances together, or similar features together. For example, keep "Director" "Next" and "Make Call" adjacent on the same Aux button row. Do not split like labels between the two sets of Aux buttons.
- Administer features that are not directly usable by the user, such as enhanced conference display, on the Station Form on buttons 20 to 24.
- Call appearances display 5 digits with a reserved area for a call state icon.
- Under the A menu, the first two Call Settings items allow the users to set the phone to go to the Phone screen when the phone is ringing (Go to Phone Screen on Ringing) and/or when the user is dialing (Go to Phone Screen on Dialing). In general, Avaya recommends that you set both to Yes - except for users covering many bridged appearances who may prefer to set the Go to Phone Screen on Ringing option to No. Users can change these settings for themselves using the Call Settings submenu.
- Group similar types of Aux buttons together on one page (Aux buttons 1-8 or Aux buttons 9-16) if possible.
  - If the user has bridged call appearances on Aux buttons, assign the bridged lines to Aux buttons 1-8 or to Aux buttons 9-16.
  - If the user has AD buttons, put them on the same page, if possible.
  - Keep related features on the same page of Aux buttons. For example, keep “Directory,” “Next,” and “Make call” together on the same row of Aux button labels and do not split between Aux buttons 8 and 9, which represent two different “pages.”
- Administer features that are not directly usable by the user, such as enhanced conference display on the Station form on buttons 20 to 24.
- Call appearances display 5 digits with a reserved area for a call state icon.

Special Considerations for the 9670G IP Telephone

The 9670G IP Telephone supports a "Quick Touch" panel that provides ease of access to any additional call appearances or switch features programmed on any of eight Quick Touch buttons. The Quick Touch panel is located at the bottom of the screen below the application area. The panel is distinguished visibly from the application area and serves as a container for the Quick Touch buttons.

Quick Touch buttons are similar to the 9650's Aux buttons. Quick Touch buttons are on-screen objects that contain a text label and can have an associated graphic (icon) to indicate the status of the button's assigned feature; the available space is 8-9 characters. If the button is a call appearance, the status icon is on the left side; otherwise the status icon is on the right side.

The basic appearance of a Quick Touch button resembles an actual physical button, and provides appropriate "pressed" (down) and "not pressed" (up) appearances.

The Quick Touch Panel supports a maximum of eight Quick Touch buttons, arranged in two rows of up to four buttons each. Only buttons with assigned features are displayed, populated from left to right starting in the top row.

The Quick Touch Panel is displayed on the Phone screen call appearance list and the Personalizing button labels option, when enabled by the associated user option (Home-> Settings-> Options & Settings-> Screen & Sounds-> Show Quick-Touch Panel), even if it contains 0 buttons. If all or any buttons are empty, that should indicate to the user that some configuration or administration needs to be done.

Shuffling

Administer shuffling on three forms:

- Feature-Related Parameters form, shown in Figure 10. Set the **Direct IP-IP Audio Connections?** field to **y** (yes).
- IP Network Region form, shown in Figure 14. Set both the **Intra-region IP-IP Direct Audio** field and the **Inter-region IP-IP Direct Audio** field to **y** (yes).
- Station form, shown in Figure 7. Set the **Direct IP-to-IP Audio Connection** to **y** (yes). The Station form setting overrides the network region, which overrides the system setting.

Wide Band Codecs

You must administer wide band codecs for each IP codec set and for IP network regions. See Appendix C: Sample Administration Forms for sample screens.

Chapter 5: Server Administration

Software Checklist

Ensure that you own licenses to use the DHCP, HTTP, and HTTPS server software.

Note:

You can install the DHCP and HTTP server software on the same machine.

CAUTION:

The firmware in the 9600 Series IP Telephones reserves IP Addresses of the form **192.168.2.x** for internal communications. The telephone(s) improperly use addresses you specify if they are of that form.

DHCP and File Servers

Dynamic Host Configuration Protocol (DHCP) minimizes maintenance for a 9600 Series IP Telephone network by removing the need to individually assign and maintain IP Addresses and other parameters for each IP telephone on the network.

The DHCP server provides the following information to the 9600 Series IP Telephones:

- IP Address of the 9600 Series IP Telephone(s)
- IP Address of the Gatekeeper board on the Avaya Media Server
- IP Address of the HTTP or HTTPS server
- The subnet mask
- IP Address of the router
- DNS Server IP Address

Administer the LAN so each IP telephone can access a DHCP server that contains the IP Addresses and subnet mask.

The IP telephone cannot function without an IP Address. The failure of a DHCP server at boot time leaves all the affected telephones unusable. A user can manually assign an IP Address to an IP telephone. When the DHCP server finally returns, the telephone never looks for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process.

Avaya recommends that:

- A minimum of two DHCP servers be available for reliability.
- A DHCP server be available when the IP telephone reboots.
- A DHCP server be available at remote sites if WAN failures isolate IP telephones from the central site DHCP server(s).

The file server provides the 9600 Series IP Telephone with a script file and, if appropriate, new or updated application software. See Step 3: Telephone and File Server on page 21 under Telephone Initialization Process. In addition, you can edit an associated settings file to customize telephone parameters for your specific environment. For more information, see Chapter 7: Administering Telephone Options.

DHCP Server Administration

This document concentrates on the simplest case of the single LAN segment. Information provided here can be used for more complex LAN configurations.

CAUTION:
Before you start, understand your current network configuration. An improper installation will cause network failures or reduce the reliability and performance of your network.

Configuring DHCP for 9600 Series IP Telephones

To administer DHCP option 242, make a copy of an existing option 176 for your 46xx IP Telephones. You can then either:

- leave any parameters the 9600 Series IP Telephones do not support for setting via DHCP in option 242 to be ignored, or
- delete unused or unsupported 9600 IP Series Telephone parameters to shorten the DHCP message length.

Only the following parameters can be set in the DHCP site-specific option for 96xx telephones, although most of them can be set in a 46xxsettings.txt file as well.

Table 8: Parameters Set by DHCP in a Site-Specific Option

Parameter	Description
DOT1X	Controls the operational mode for 802.1X. The default is 0 (pass-through of multicast EAPOL messages to an attached PC, and enable Supplicant operation for unicast EAPOL messages).
DOT1XSTAT	Controls 802.1X Supplicant operation.
HTTPDIR	Specifies the path name to prepend to all file names used in HTTP and HTTPS GET operations during startup. (0 to 127 ASCII characters, no spaces.) The command is "**`SET HTTPDIR myhttpdir`**". The path (relative to the root of the TLS or HTTP file server) where 96xx telephone files are stored. If an Avaya file server is used to download configuration files over TLS, but a different server is used to download software files via HTTP, set the path of the Avaya server in the DHCP site-specific option, and set HTTPDIR again in the 46xxsettings.txt file with the appropriate path for the second server. HTTPDIR is the path for all HTTP operations **except** for BRURI.
HTTPPORT	Specifies the TCP port number to be used for HTTP file downloading.
HTTPSRVR	IP Address(es) or DNS name(s) of HTTP file server(s) used to download 96xx telephone software files. The files are digitally signed, so TLS is not required for security.
ICMPDU	Controls the extent to which ICMP Destination Unreachable messages are sent in response to messages sent to closed ports so as not to reveal information to potential hackers. The default is 1 (sends Destination Unreachable messages for closed ports used by traceroute).
ICMPRED	Controls whether ICMP Redirect messages are processed. The default is 0 (redirect messages are not processed).
L2Q	802.1Q tagging mode. The default is 0 (automatic).
L2QVLAN	VLAN ID of the voice VLAN. The default is 0.
LOGLOCAL	Controls the severity level of events logged in the SNMP MIB. The default is 7.
MCIPADD	CM server(s) IP Address(es) or DNS name(s). If there are too many addresses or names to include all of them in the DHCP site-specific option, include at least one from each major system. Then set MCIPADD again in the 46xxsettings.txt file with the complete list of addresses. Providing a subset of the addresses via DHCP improves reliability if the file server is not available due to server or network problems.
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 (auto-negotiate).
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 (auto-negotiate).
PROCPSWD	Security string used to access local procedures. The default is 27238 (CRAFT).
PROCSTAT	Controls whether local (Craft) procedures are allowed. The default is 0 (access to all administrative options is allowed).
SNMPADD	Allowable source IP Address(es) for SNMP queries. The default is " " (Null).
SNMPSTRING	SNMP community name string. The default is " " (Null).
STATIC	Controls whether to use a manually-programmed file server or CM IP Address instead of those received via DHCP or a settings file. If a manually-programmed file server IP Address is to be used, STATIC **must** be set via DHCP.
TLSDIR	Specifies the path name prepended to all file names used in HTTPS GET operations during startup.
TLSPORT	Specifies the TCP port number used for HTTPS file downloading.

Table 8: Parameters Set by DHCP in a Site-Specific Option (continued)

Parameter	Description
TLSSRVR	IP Address(es) or DNS name(s) of Avaya file server(s) used to download configuration files. **Note:** Transport Layer Security is used to authenticate the server.
TLSSRVRID	Controls whether the identity of a TLS server is checked against its certificate.
VLANTEST	Controls the length of time the telephone tries DHCP with a non-zero VLAN ID. When the interval is exceeded, the telephone records the VLAN ID so that it is not used again, and DHCP continues on the default VLAN. The default is 60 seconds.

The parameters in Table 8 are saved in a 9600 Series IP Telephone's non-volatile memory. If the DHCP server is not available for any reason during telephone restart or reboot, the telephone uses these saved parameters.

DHCP Generic Setup

This document is limited to describing a generic administration that works with the 9600 Series IP Telephones. Three DHCP software alternatives are common to Windows operating systems:

- Windows NT® 4.0 DHCP Server
- Windows 2000® DHCP Server
- Windows 2003® DHCP Server

Any other DHCP application might work. It is the responsibility of the customer to install and configure the DHCP server correctly.

DHCP server setup involves:

1. Installing the DHCP server software according to vendor instructions.
2. Configuring the DHCP server with:
   - IP Addresses available for the 9600 Series IP Telephones.
   - The following DHCP options:
     - **Option 1 - Subnet mask**.
       As described in Table 3, item 3.
     - **Option 3 - Gateway (router) IP Address(es)**.
       As described in Table 3, item 1. If using more than one address, the total list can contain up to 255 total ASCII characters. You must separate IP Addresses with commas with no intervening spaces.
     - **Option 6 - DNS server(s) address list**.
       If using more than one address, the total list can contain up to 127 total ASCII characters. You must separate IP Addresses with commas with no intervening spaces. At least one address in Option 6 must be a valid, non zero, dotted decimal address.

- **Option 12 - Host Name**.
  Value is **AV*ohhhhhh***, where: *o* is “A” if the OID (first three octets) of the MAC address for the telephone is 00-04-0D, “B” if the OID is 00-1B-4F, “E” if the OID is 00-09-6E, “L” if the OID is 00-60-1D, “T” if the OID is 00-07-3B, and “X” if the OID is anything else and where *hhhhhh* are ASCII characters for the hexadecimal representation of the last three octets of the MAC address for the telephone.
- **Option 15 - DNS Domain Name**.
  This string contains the domain name to be used when DNS names in system parameters are resolved into IP Addresses. This domain name is appended to the DNS name before the 9600 IP Telephone attempts to resolve the DNS address. Option 15 is necessary if you want to use a DNS name for the HTTP server. Otherwise, you can specify a DOMAIN as part of customizing HTTP as indicated in DNS Addressing on page 103.
- **Option 51 - DHCP lease time**.
  If this option is not received, the DHCPOFFER is not be accepted. Avaya recommends a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the IP Address lease is assumed to be infinite as per RFC 2131, Section 3.3, so that renewal and rebinding procedures are not necessary even if Options 58 and 59 are received. Expired leases cause Avaya IP Telephones to reboot. Avaya recommends providing enough leases so an IP Address for an IP telephone does not change if it is briefly taken offline.

Note:

The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP Address. If the network has problems and the only DHCP server is centralized, the server is not accessible to the given telephone. In this case the telephone is not usable until the server can be reached.
Avaya recommends, once assigned an IP Address, the telephone continues using that address after the DHCP lease expires, until a conflict with another device is detected. As Table 11: 9600 Series IP Telephone Customizable System Parameters indicates, the system parameter DHCPSTD allows an administrator to specify that the telephone will either:
a). Comply with the DHCP standard by setting DHCPSTD to “1”, or
b). Continue to use its IP Address after the DHCP lease expires by setting DHCPSTD to “0.”

The latter case is the default. If the default is invoked, after the DHCP lease expires the telephone sends an ARP Request for its own IP Address every five seconds.
The request continues either forever, or until the telephone receives an ARP Reply. After receiving an ARP Reply, the telephone displays an error message, sets its IP Address to 0.0.0.0, and attempts to contact the DHCP server again.

- **Option 52 - Overload Option, if desired**.
  If this option is received in a message, the telephone interprets the **sname** and **file**

fields in accordance with IETF RFC 2132,
Section 9.3, listed in Appendix B: Related Documentation.

- **Option 53 - DHCP message type**.
  Value is 1 (DHCPDISCOVER) or 3 (DHCPREQUEST).
- **Option 55 - Parameter Request List**.
  Acceptable values are:
  1 (subnet mask),
  3 (router IP Address[es])
  6 (domain name server IP Address[es])
  15 (domain name)
  NVSSON (site-specific option number)
- **Option 57 - Maximum DHCP message size**.
  Prior to 9600 Series IP Telephone Software Release 3.0, the maximum size is 576 octets. As of Release 3.0, the maximum size is 1,000 octets.
- **Option 58 - DHCP lease renew time**.
  If not received or if this value is greater than that for Option 51, the default value of T1 (renewal timer) is used as per IETF RFC 2131, Section 4.5, listed in Related Documentation.
- **Option 59 - DHCP lease rebind time**.
  If not received or if this value is greater than that for Option 51, the default value of T2 (rebinding timer) is used as per RFC 2131, Section 4.5
- **Option 60 - Vendor Class identifier**.
  The default value is "ccp.avaya.com" and all values must be at most 13 characters in length.

The 9600 Series IP Telephones do not support Regular Expression Matching, and therefore, do not use wildcards. For more information, see Administering Options for the 9600 Series IP Telephones on page 85.

In configurations where the upgrade script and application files are in the default directory on the HTTP server, do not use the HTTPDIR=<path>.

You do not have to use Option 242. If you do not use this option, you must ensure that the key information, especially HTTPSRVR and MCIPADD, is administered appropriately elsewhere.

Avaya recommends that you administer DHCP servers to deliver only the options specified in this document. Administering additional, unexpected options might have unexpected results, including causing the IP telephone to ignore the DHCP server.

The DHCP server name and HTTP server name must each be no more than 32 characters in length.

Examples of good DHCP administration include:

- Option 6: “***aaa.aaa.aaa.aaa***”
- Option 15: “***yourco.com***”

- Option 242: “**MCIPADD=*xxxx.xxx.xxx.xxx***”

  Depending on the DHCP application you choose, be aware that the application most likely does not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client a day or more. For example, Windows NT® DHCP reserves expired leases for about one day. This reservation period protects a lease for a short time. If the client and the DHCP server are in two different time zones, the clocks of the computers are not in sync, or the client is not on the network when the lease expires, there is time to correct the situation.

  The following example shows the implication of having a reservation period: Assume two IP Addresses, therefore two possible DHCP leases. Assume three IP telephones, two of which are using the two available IP Addresses. When the lease for the first two telephones expires, the third telephone cannot get a lease until the reservation period expires. Even if the other two telephones are removed from the network, the third telephone remains without a lease until the reservation period expires.

In Table 9, the 9600 Series IP Telephone sets the system values to the DHCPACK message field values shown.

Table 9: DHCPACK Setting of System Values

System Value	Set to
IPADD	The **yiaddr** field.
EXTIPADD	The **yiaddr** field; VPN mode only - external ("outer") IP address of the telephone in VPN mode.
NETMASK	Option #1 (if received).
EXTNETMASK	Option #1; VPN mode only - external ("outer") subnet mask in VPN mode.
GIPADD	Option #3 (if received, which might be a list of IP Addresses).
EXTGIPADD	Option #3; VPN mode only - external ("outer") router IP address(es) in VPN mode.
TLSSRVR	The **siaddr** field, if that field is non-zero.
HTTPSRVR	The **siaddr** field, if that field is non-zero.
DNSSRVR	Option #6 (if received, which might be a list of IP Addresses).
EXTDNSSRVR	Option #6; VPN mode only - eExternal ("outer") DNS server IP address(es) in VPN mode.
DOMAIN	Option #15 (if received).
DHCP lease time	Option #51 (if received).

Table 9: DHCPACK Setting of System Values (continued)

System Value	Set to
DHCP lease renew time	Option #58 (if received).
DHCP lease rebind time	Option #59 (if received).

The system values L2Q, L2QVLAN, and PHY2VLAN are not set from a *name=value* pair if those system values were previously set by LLDP. For more information, see Link Layer Discovery Protocol (LLDP).

Since the site-specific option is processed after the DHCP fields and standard options, any values set in the site-specific option (Option #242) will supersede any values set via DHCP fields or standard options, as well as any other previously set values. Examples of values that can be set using Option #242 are as follows:

- HTTPDIR
- HTTPPORT
- STATIC
- TLSDIR
- TLSPORT
- TLSSRVRID
- DOT1X
- DOT1XSTAT
- ICMPDU
- ICMPRED
- L2Q
- L2QVLAN
- LOGLOCAL
- PHY1STAT
- PHY2STAT
- PROCPSWD
- PROCSTAT
- SNMPADD
- SNMPSTRING
- SNMPTEST
- VLANTEST

Windows NT 4.0 DHCP Server

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**-->**Settings**-->**Control Panel**.
2. Double-click the **Network** icon.
3. Verify that **Microsoft DHCP Server** is listed as one of the Network Services on the **Services** tab.
4. If it is listed, continue with the next section. If it is not listed, install the DHCP server.

Creating a DHCP Scope for the IP Telephones

Use the following procedure to create a DHCP scope for the IP telephones.

1. Select **Start**-->**Programs**-->**Admin Tools**-->**DHCP Manager**.
2. Expand **Local Machine** in the DHCP Servers window by double clicking it until the **+** sign changes to a **-** sign.
3. Select **Scope**-->**Create**.
4. Using information recorded in Table 3: Required Network Information Before Installation - Per DHCP Server:

   Define the **Telephone IP Address Range**.

   Set the **Subnet Mask**.

   To ***exclude*** any IP Addresses you do not want assigned to IP telephones within the **Start** and **End** addresses range:

   a. In the **Exclusion Range Start Address** field, enter the ***first IP Address*** in the range that you want to exclude.

   b. In the **Exclusion Range End Address** field, enter the ***last IP Address*** in the range that you want to exclude.

   c. Click the **Add** button.

   d. Repeat steps a. through c. for each IP Address range to be excluded.

   Note:

   Avaya recommends that you provision the 9600 Series IP Telephones with sequential IP Addresses. Also do not mix 9600 Series IP Telephones and PCs in the same scope.

5. Under **Lease Duration**, select the **Limited To** option and set the ***lease duration*** to the maximum.

6. Enter a ***sensible name*** for the **Name** field, such as “CM IP Telephones," where CM would represent Avaya Communication Manager.
7. Click **OK**.

   A dialog box prompts you: `Activate the new scope now?`
8. Click **No**.

Note:

Activate the scope only after setting all options.

Editing Custom Options

Use the following procedure to edit custom options.

1. Highlight the newly created scope.
2. Select **DHCP Options**-->**Defaults** in the menu.
3. Click the **New** button.
4. In the **Add Option Type** dialog box, enter an appropriate custom option name, for example, “9600OPTION.”
5. Change the **Data Type Byte** value to **String**.
6. Enter **242** in the **Identifier** field.
7. Click the **OK** button.

   The **DHCP Options** menu displays.
8. Select the **Option Name** for 242 and set the *value string*.
9. Click the **OK** button.
10. For the **Option Name** field, select **003 Router** from the drop-down list.
11. Click **Edit Array**.
12. Enter the ***Gateway IP Address*** recorded in Table 3: Required Network Information Before Installation - Per DHCP Server for the **New IP Address** field.
13. Select **Add** and then **OK**.

Adding the DHCP Option

Use the following procedure to add the DHCP option.

1. Highlight the scope you just created.
2. Select **Scope** under **DHCP Options**.
3. Select the **242** option that you created from the **Unused Options** list.
4. Click the **Add** button.

5. Select option **003** from the **Unused Options** list.
6. Click the **Add** button.
7. Click the **OK** button.
8. Select the **Global parameter** under **DHCP Options**.
9. Select the **242** option that you created from the **Unused Options** list.
10. Click the **Add** button.
11. Click the **OK** button.

Activating the Leases

Use the following procedure to activate the leases.

- Click **Activate** under the **Scope** menu.
  The light-bulb icon for the scope lights.

Verifying Your Configuration

This section describes how to verify that the **96XXOPTIONs** are correctly configured for the Windows NT® 4.0 DHCP server.

Note:

Although this configuration represents that for 9600 Series IP Telephones, the file remains as 46XXOPTIONS. This allows shared use for both 4600 and 9600 Series IP Telephones.

Verify the Default Option, 242 96XXOPTION

1. Select **Start**-->**Programs**-->**Admin Tools**-->**DHCP Manager**.
2. Expand **Local Machine** in the DHCP servers window by double clicking until the **+** sign changes to a **-** sign.
3. In the DHCP servers frame, click the *scope* for the IP telephone.
4. Select **Defaults** from the **DHCP_Options** menu.
5. In the **Option Name** pull-down list, select **242 96XXOPTION**.
6. Verify that the **Value String** box contains the correct string from DHCP Server Administration.
   If not, update the string and click the **OK** button twice.

Verify the Scope Option, 242 96XXOPTION

1. Select **Scope** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 96XXOPTION**.
3. Click the **Value** button.

4. Verify that the **Value String** box contains the correct string from The parameters in Table 8 are saved in a 9600 Series IP Telephone's non-volatile memory. If the DHCP server is not available for any reason during telephone restart or reboot, the telephone uses these saved parameters. on page 58.
   If not, update the string and click the **OK** button.

Verify the Global Option, 242 96XXOPTION

1. Select **Global** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 96XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct value from The parameters in Table 8 are saved in a 9600 Series IP Telephone's non-volatile memory. If the DHCP server is not available for any reason during telephone restart or reboot, the telephone uses these saved parameters. on page 58. If not, update the string and click the **OK** button.

Windows 2000 DHCP Server

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**-->**Program**-->**Administrative Tools**-->**Computer Management**.
2. Under **Services and Applications** in the Computer Management tree, find **DHCP**.
3. If DHCP is not installed, install the DHCP server. Otherwise, proceed directly to Creating and Configuring a DHCP Scope for instructions on server configuration.

Creating and Configuring a DHCP Scope

Use the following procedure to create and configure a DHCP scope.

1. Select **Start**-->**Programs**-->**Administrative Tools**-->**DHCP**.
2. In the console tree, click the *DHCP server* to which you want to add the DHCP scope for the IP telephones. This is usually the name of your DHCP server machine.
3. Select **Action**-->**New Scope** from the menu.
   Windows displays the **New Scope Wizard** to guide you through rest of the setup.
4. Click the **Next** button.
   The **Scope Name** dialog box displays.
5. In the **Name** field, enter a name for the scope such as "CM IP Telephones" (where CM would represent Avaya Communication Manager), then enter a brief comment in the **Description** field.
6. When you finish Steps 1 - 5, click the **Next** button.
   The **IP Address Range** dialog box displays.

7. Define the range of IP Addresses used by the IP telephones listed in Table 3: Required Network Information Before Installation - Per DHCP Server. The **Start IP Address** is the first IP Address available to the IP telephones. The **End IP Address** is the last IP Address available to the IP telephones.

   Note:

   Avaya recommends not mixing 9600 Series IP Telephones and PCs in the same scope.

8. Define the **subnet mask** in one of two ways:

   - The number of bits of an IP Address to use for the network/subnet IDs.
   - The subnet mask IP Address.

   Enter only one of these values. When you finish, click the **Next** button.

   The **Add Exclusions** dialog box displays.

9. Exclude any IP Addresses in the range specified in the previous step that you do not want assigned to an IP telephone.

   a. In the **Start Address** field under **Exclusion Range**, enter the ***first IP Address*** in the range you want to exclude.
   b. In the **End Address** field under **Exclusion Range**, enter the ***last IP Address*** in the range you want to exclude.
   c. Click the **Add** button.
   d. Repeat steps a. through c. for each IP Address range that you want to exclude.

   Note:

   You can add additional exclusion ranges later by right clicking the **Address Pool** under the newly created scope and selecting the **New Exclusion Range** option.

   Click the **Next** button after you enter all the exclusions.
   The **Lease Duration** dialog box displays.

10. For all telephones that obtain their IP Addresses from the server, enter **30 days** in the **Lease Duration** field. This is the duration after which the IP Address for the device expires and which the device needs to renew.

11. Click the **Next** button.
    The **Configure DHCP Options** dialog box displays.

12. Click the **No, I will activate this scope later** button.
    The **Router** (Default Gateway) dialog box displays.

13. For each router or default gateway, enter the ***IP Address*** and click the **Add** button.
    When you are done, click the **Next** button.
    The **Completing the New Scope Wizard** dialog box displays.

14. Click the **Finish** button.
    The new scope appears under your server in the DHCP tree. The scope is not yet active and does not assign IP Addresses.

15. Highlight the newly created scope and select **Action**-->**Properties** from the menu.

16. Under **Lease duration for DHCP clients**, select **Unlimited** and then click the **OK** button.

    CAUTION:

    IP Address leases are kept active for varying periods of time. To avoid having calls terminated suddenly, make the lease duration unlimited.

Adding DHCP Options

Use the following procedure to add DHCP options to the scope you created in the previous procedure.

1. On the DHCP window, right-click the **Scope Options** folder under the scope you created in the last procedure.

   A drop-down menu displays.

2. In the left pane of the DHCP window, right click the **DHCP Server name**, then click **Set Predefined Options...**.
3. Under **Predefined Options and Values**, click **Add**.
4. In the **Option Type Name** field, enter ***any appropriate name***, for example, “Avaya IP Telephones.”
5. Change the **Data Type** to **String**.
6. In the **Code** field, enter **242**, then click the **OK** button twice.

   The **Predefined Options and Values** dialog box closes, leaving the DHCP dialog box enabled.

7. Expand the newly created scope to reveal its **Scope Options**.
8. Click **Scope Options** and select **Action**-->**Configure Options** from the menu.
9. In the **General** tab page, under the **Available Options**, check the **Option 242** checkbox.
10. In the **Data Entry** box, enter the ***DHCP IP telephone option string*** as described in The parameters in Table 8 are saved in a 9600 Series IP Telephone’s non-volatile memory. If the DHCP server is not available for any reason during telephone restart or reboot, the telephone uses these saved parameters. on page 58.

    Note:

    You can enter the text string directly on the right side of the **Data Entry** box under the ASCII label.

11. From the list in **Available Options**, check option **003 Router**.
12. Enter the ***gateway (router) IP Address*** from the IP Address field of Table 3: Required Network Information Before Installation - Per DHCP Server.
13. Click the **Add** button.
14. Click the **OK** button.

Activating the New Scope

Use the following procedure to activate the new scope.

1. In the DHCP console tree, click the **IP Telephone Scope** you just created.
2. From the **Action** menu, select **Activate**.

   The small red down arrow over the scope icon disappears, indicating that the scope was activated.

HTTP Generic Setup

You can store the same application software, script file, and settings file on an HTTP server as you can on a TFTP server. TFTP is not supported for 9600 Series IP Telephones. With proper administration, the telephone seeks out and uses that material. Some functionality might be lost by a reset if the HTTP server is unavailable. For more information, see DHCP and File Servers on page 55.

CAUTION:

The files defined by HTTP server configuration must be accessible from all IP telephones invoking those files. Ensure that the file names match the names in the upgrade script, including case, since UNIX systems are case-sensitive.

Note:

Use any HTTP application you want. Commonly used HTTP applications include Apache® and Microsoft® IIS™.

Important:

You must use the Avaya Web configuration server to obtain HTTPS so information is authenticated.

The Avaya Web configuration server does not support backup/restore. If you intend to use HTTP for backup/restore purposes, you must use an HTTP server that is independent of the Avaya Web configuration server.

To set up an HTTP server:

- Install the HTTP server application.
- Administer the system parameters HTTPSRVR and CODESRVR to the address(es) of the HTTP server. Include these parameters in DHCP Option 242, or the appropriate SSON Option.
- Download the upgrade script file and application file(s) from the Avaya Web site http://www.avaya.com/support to the HTTP server. For more information, see Contents of the Settings File on page 82.

Note:

Many LINUX servers distinguish between upper and lower case names. Ensure that you specify the settings file name accurately, as well as the names and values of the data within the file.

If you choose to enhance the security of your HTTP environment by using Transport Layer Security (TLS), you also need to:

- Install the TLS server application.
- Administer the system parameter TLSSRVR to the address(es) of the Avaya HTTP server.

HTTP/HTTPS Configuration for Backup/Restore

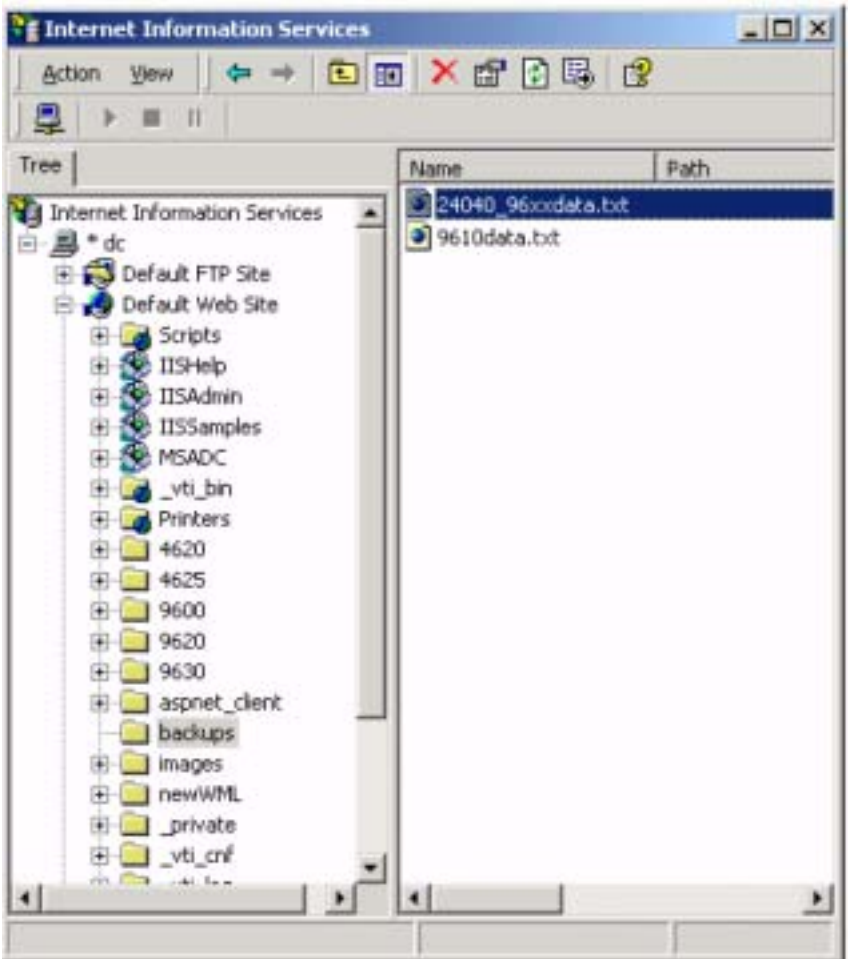
In addition to the procedures in this section, you can use the Avaya File Server Application for configuration, firmware file download, and backup/restore. You can download this application from http://www.avaya.com/support.

For IIS Web Servers

Important:

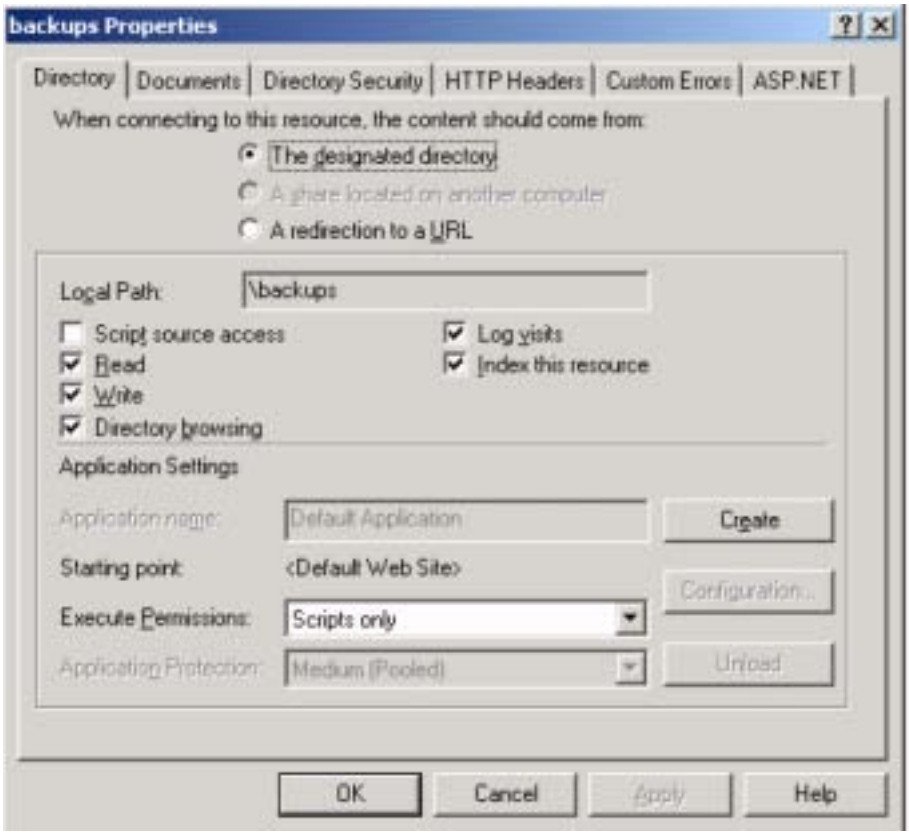
You must have accounts in the domain of your IIS server.

3. Go to **control panel/Administrative Tools/Internet Services Manager** and select the directory you created to hold the backups.

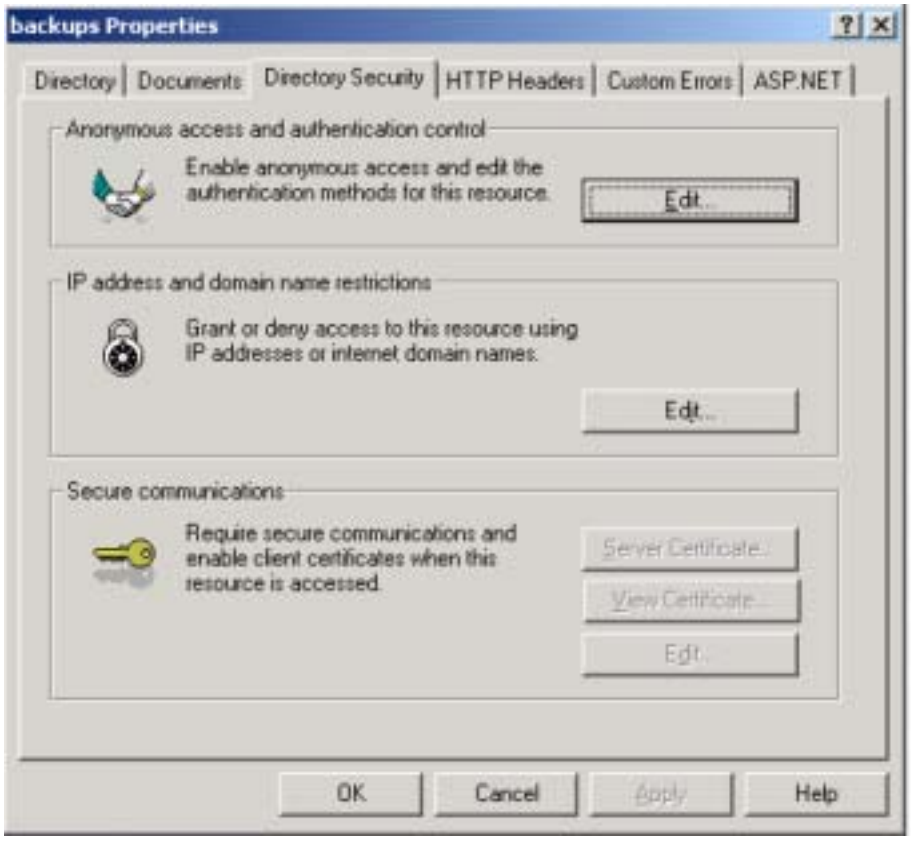


4. Right click and select **Properties**.

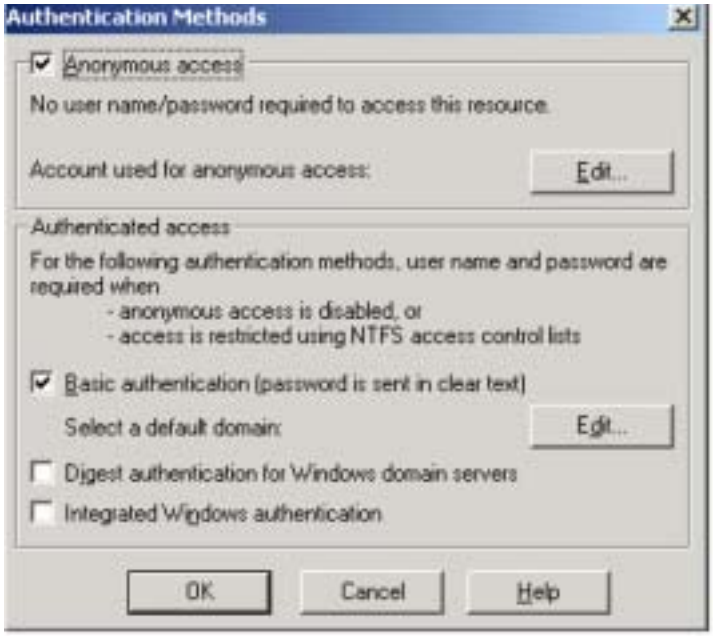
5. Select **Directory** and enable write access.



6. Select **Directory Security**.



7. Select **Directory Security/Anonymous access** and **authentication control/Edit**.


Authentication Methods
Anonymous access
No user name/password required to access this resource.
Account used for anonymous access:
Edit...
Authenticated access
For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists
Basic authentication (password is sent in clear text)
Select a default domain:
Edit...
Digest authentication for Windows domain servers
Integrated Windows authentication
OK
Cancel
Help

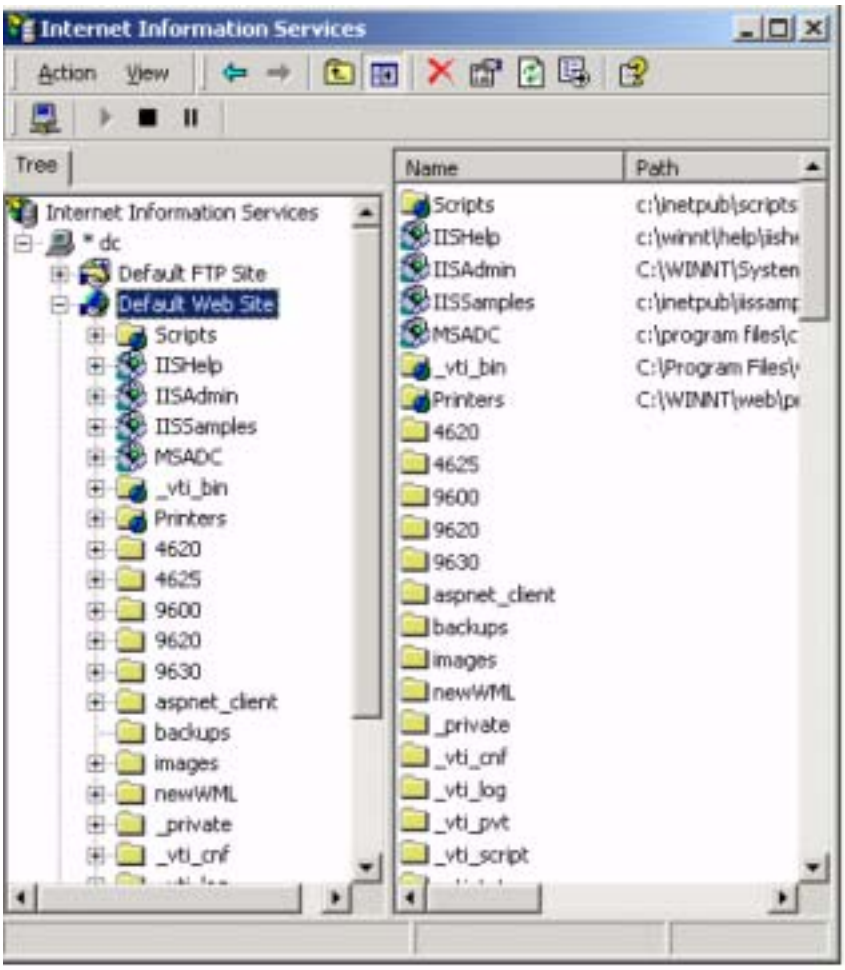
8. Select **Basic authentication** (password is sent in clear text).
9. Click **Edit** next to Select a default domain:

Basic Authentication Domain
Basic Authentication Domain
The default Windows Domain used for Basic Authentication is the local domain the web server is active in. If the default domain should be other than the local domain, enter it here.
Domain Name:
Browse...
Use Default
OK
Cancel
Help

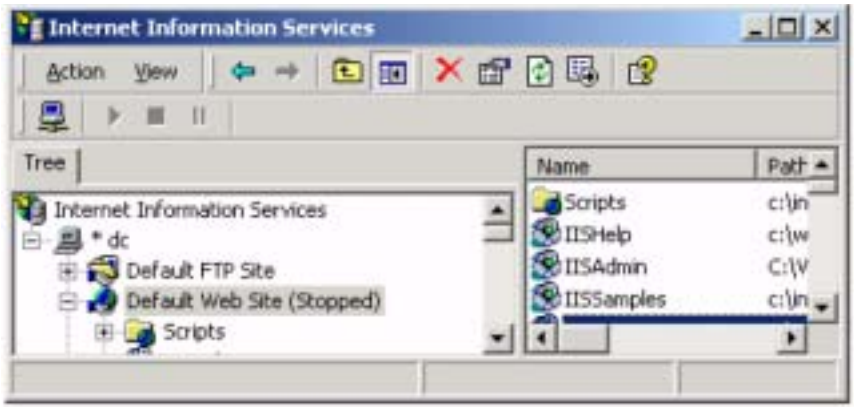
The domain name should be blank.

10. Press **OK** several times to accept your settings.

11. Stop and restart the Web server. Right click on the default Web server.

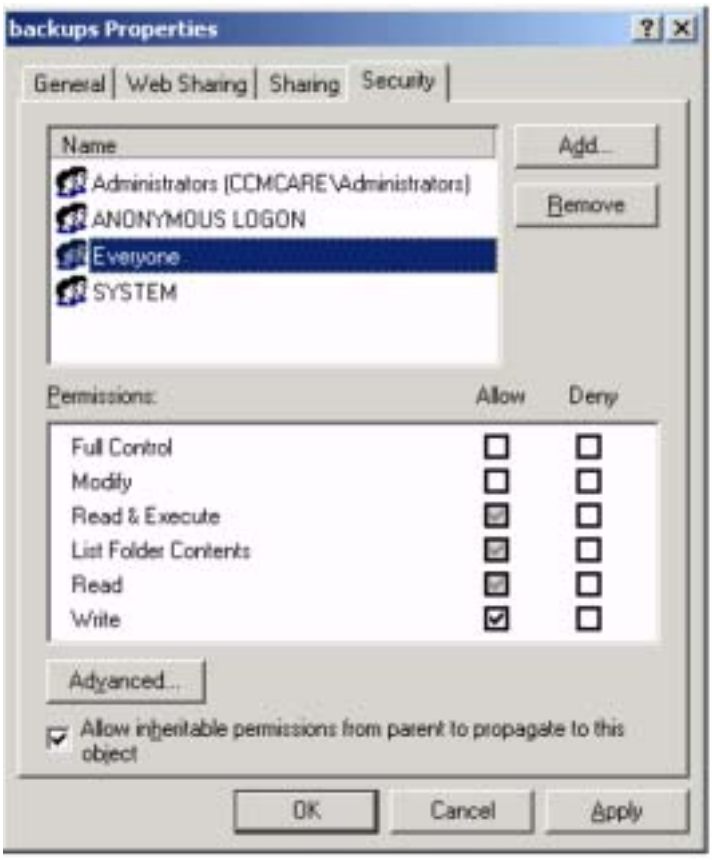


12. Select **Stop**.



13. Right click again and Select **Start**.

14. Open Explorer and find the directory. Right click and open properties. Ensure that all of your telephone users have write permission in this directory.



15. Now have your users do a manual backup. They will be prompted for their user id and password.

    When each backup completes successfully, the telephone will remember the userid and password and automatic backups will proceed normally.

For Apache Web Servers

1. Create a “backup” folder under the root directory of your Web server, and **make the folder writable by everyone**. All backup files will be stored in that directory.

   If your backup folder is for instance **C:/Program Files/Apache Group/Apache2/htdocs/backup**, the 46xxsettings.txt file should have a line similar to:

   [SET BRURI http://www.website.com/backup/]

   If your backup folder is the root directory, the 46xxsettings.txt file should have a line similar to:

   [SET BRURI http://www.website.com/]

2. Edit your Web server configuration file **httpd.conf**.
3. Uncomment the two LoadModule lines associated with DAV:

   ```
   LoadModule dav_module modules/mod_dav.so
   LoadModule dav_fs_module modules/mod_dav_fs.so
   ```

   Note:

   If these modules are not available on your system, typically the case on some Unix/Linux Apache servers, you have to recompile these two modules (mod_dav & mod_dav_fs) into the server. Other ways to load these modules might be available. Check your Apache documentation at http://httpd.apache.org/docs/ for more details.

4. Add the following lines in the **httpd.conf** file:

   ```
   #
   # WebDAV configuration
   #
   DavLockDB "C:/Program Files/Apache Group/Apache2/var/DAVLock"
     <Location />
     Dav On
     </Location>
   ```

   For Unix/Linux Web servers the fourth line might look more like:

   ```
   DavLockDB/usr/local/apache2/var/DAVLock
   ```

5. Create the var directory and **make it writable by everyone**. Right click **Properties**-->**Security**-->**Add**-->**Everyone**-->**Full Control**.

Internal Audio Parameters

The system parameter AUDIOENV provides control of some internal audio parameters. Avaya does not recommend that customers set these values. In certain situations, particularly noisy environments, Avaya SSE may recommend a change in the AUDIOENV setting to reduce/ eliminate the effects environmental noise can have during telephone use. AUDIOENV is an index into a table that impacts four internal variables:

Table 10: Internal Audio Variables

Variable	Description	Possible Values
AGC_Dyn_Range	AGC dynamic range.	0 for a typical office environment (+/-9dB), 1 for +/-12dB, 2 for +/-15dB, and 3 for +/-18 AGC Dynamic range variation.
NR_thresh_Hd	The noise reduction threshold for the headset.	The noise reduction threshold for the headset has a default value of 0 for a typical office environment, 1 for call center applications, 2 and 4 for increasingly noisy audio environments, and 3 where noise reduction is disabled.
NR_thresh_Hs	The noise reduction threshold for the handset.	The noise reduction threshold for the handset has a default value of 0 for a typical office environment, 1 for call center applications, 2 and 4 for increasingly noisy audio environments, and 3 where noise reduction is disabled.
HD_Tx_Gain	Headset transmit gain.	Headset transmit gain has a default value of 0 for normal transmit gain, 1 for +6dB of gain, and 2 for -6dB of gain.

AUDIOENV= a range of 0 to 299 beginning with Release 2.0. Set AUDIOENV 0 is the nominal setting (0,0,0,0).

For more information, see *Audio Quality Tuning for IP Telephones, Issue 2* on www.avaya.com/support.

Chapter 6: Telephone Software and Application Files

General Download Process

The 9600 Series IP Telephones download upgrade files, settings files, language files, certificate files, and software files from a file server. All of the file types can be downloaded either via HTTP or HTTPS except the software files, which can only be downloaded via HTTP. Avaya recommends HTTPS for downloading the non-software file types because it ensures the integrity of the downloaded file by preventing "man in the middle" attacks. Further, once the trusted certificates are downloaded into the telephone, HTTPS ensures that the file server itself will be authenticated via a digital certificate. HTTPS is not used for software file downloads because 9600 Series IP Telephone software files are already digitally signed, so there is no need to incur additional processing overhead while downloading these relatively large files. The HTTPS protocol applies only if the server supports Transport Layer Security (TLS) encryption.

Note:

The 96xxupgrade.txt file, binary files, and settings files discussed in this chapter are identical for file servers running HTTP and HTTPS. The generic term “file server” refers to a server running either HTTP or HTTPS.

When shipped from the factory, 9600 Series IP Telephones might not contain the latest software. When the telephone is first plugged in, it will attempt to contact a file server, and will download new software if the software version available on the file server is different than the version on the phone. For subsequent software upgrades, the call server provides the capability to remotely reset the telephone, which then initiates the same process for contacting a file server.

The telephone queries the file server, which transmits a 96xxupgrade.txt file to the telephone. The 96xxupgrade.txt file tells the telephone which binary file the telephone must use. The binary file is the software that has the telephony functionality, and is easily updated for future enhancements. In a newly installed telephone, the binary file might be missing. In a previously installed telephone, the binary file might not be the proper one. In both cases, the telephone requests a download of the proper binary file from the file server. The file server downloads the file and conducts some checks to ensure that the file was downloaded properly. If the telephone determines it already has the proper file, the telephone proceeds to the next step without downloading the binary file again.

After checking and loading the binary file, the 9600 Series IP Telephone, if appropriate, uses the 96xxupgrade.txt file to look for a settings file. The settings file contains options you have administered for any or all of the IP Telephones in your network. For more information about the settings file, see Contents of the Settings File on page 82.

9600 Series IP Telephone Scripts and Application Files

Choosing the Right Application File and Upgrade Script File

The software releases containing the files needed to operate the 9600 Series IP Telephones are bundled together. You download this self-extracting executable file to your file server from the Avaya support Web site at: http://www.avaya.com/support. The file is available in both zipped and unzipped format.

The bundle contains:

- An upgrade script file and a settings file, which allow you to upgrade to new software releases and new functionality without having to replace IP telephones.
- Application files for all current 9600 Series IP Telephones.
- Other useful information such as a ReadMe file and a settings file template to customize parameters and settings, and the latest binary code.
- As of software Release 2.0, all 96xx telephone software distribution packages include a file containing a copy of the Avaya Product Root Certificate Authority certificate. All downloadable trusted certificate files are in PEM (Privacy-Enhanced Mail) format, as specified in section A.1 of Appendix A of RFC 1422.

Upgrade Script File

An upgrade script file tells the IP telephone whether the telephone needs to upgrade software. The Avaya IP Telephones attempt to read this file whenever they reset. The upgrade script file also points to the settings file.

You download a default upgrade script file, sometimes called the “script file,” from http://www.avaya.com/support. This file allows the telephone to use default settings for customer-definable options. To administer customer-defined settings, you must create a file called ***46xxsettings.txt***, which resides in the same directory as the upgrade script file.

Note:

Avaya recommends that the settings file have the extension ***.txt**. The Avaya IP Telephones can operate without this file. You can also change these settings with DHCP or, in some cases, from the dialpad of the telephone.

Settings File

The settings file contains the option settings you need to customize the Avaya IP Telephones for your enterprise.

Note:

You can use one settings file for all your Avaya IP Telephones. The settings file includes the 9600 Series IP Telephones covered in this document and 4600 Series IP Telephones, as covered in the *4600 Series IP Telephone LAN Administrator Guide* (Document Number 555-233-507).

The settings file can include any of five types of statements, one per line:

- Comments, which are statements with a "#" character in the first column.
- Tags, which are comments that have exactly one space character after the initial #, followed by a text string with no spaces.
- **`Goto`** commands, of the form **GOTO *tag.*** **`Goto`** commands cause the telephone to continue interpreting the configuration file at the next line after a **# *tag*** statement. If no such statement exists, the rest of the configuration file is ignored.
- Conditionals, of the form **IF *$name* SEQ *string* GOTO *tag***. Conditionals cause the **`Goto`** command to be processed if the value of ***name*** is a case-insensitive equivalent to ***string***. If no such ***name*** exists, the entire conditional is ignored. The only system values that can be used in a conditional statement are: BOOTNAME, GROUP, and SIG.
- **SET** commands, of the form **SET *parameter_name value***. Invalid values cause the specified value to be ignored for the associated ***parameter_name*** so the default or previously administered value is retained. All values must be text strings, even if the value itself is numeric, a dotted decimal IP Address, and so on.

Note:

Enclose all data in quotation marks for proper interpretation.

The upgrade script file Avaya provides includes a line that tell the telephone to **GET *46xxsettings.txt***. This lines causes the telephone to use HTTP to attempt to download the file specified in the **`GET`** command. If the file is obtained, its contents are interpreted as an additional script file. That is how your settings are changed from the default settings. If the file cannot be obtained, the telephone continues processing the upgrade script file.

If the configuration file is successfully obtained but does not include any setting changes the telephone stops using HTTP. This happens when you initially download the script file template from the Avaya support Web site, before you make any changes. When the configuration file contains no setting changes, the telephone does not go back to the upgrade script file.

Avaya recommends that you do **not** alter the upgrade script file. If Avaya changes the upgrade script file in the future, any changes you have made will be lost. Avaya recommends that you use the ***46xxsettings*** file to customize your settings instead. However, you can change the settings file name, if desired, as long as you also edit the corresponding **`GET`** command in the upgrade script file.

For more information on customizing your settings file, see Contents of the Settings File.

Contents of the Settings File

After checking the application software, the 9600 Series IP Telephone looks for a 46xxsettings file. This optional file is where you identify non-default option settings, application-specific parameters, and so on. You can download a template for this file from the Avaya support Web site. An example of what the file might look like follows.

Note:

The following is intended only as a simple example. Your settings will vary from the settings shown. This sample assumes specification of a DNS Server, turning off enhanced local dialing, and a Web Browser.

DNSSRVR=”dnsexample.yourco.com”

ENDIALSTAT=0

WMLHOME=”http://yourco.com/home.wml”
WMLPORT=”8000”
WMLPROXY=”11.11.11.11”

See Chapter 7: Administering Telephone Options for details about specific values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

VLAN separation controls whether or not traffic received on the secondary Ethernet interface is forwarded on the voice VLAN and whether network traffic received on the data VLAN is forwarded to the telephone. Add commands to the 46xxsettings.txt file to enable VLAN separation. The following example assumes the data VLAN ID is “yyy” and the data traffic priority is “z”:

SET VLANSEP 1
SET PHY2VLAN yyy
SET PHY2PRIO z

Note:

Also configure the network switch so that 802.1Q tags are not removed from frames forwarded to the telephone.

The GROUP System Value

You might have different communities of users, all of which have the same telephone model, but which require different administered settings. For example, you might want to restrict Call Center agents from being able to Logoff, which might be an essential capability for “hot-desking” associates. We provide examples of the group settings for each of these situations later in this section.

Use the GROUP system value for this purpose:

1. identify which telephones are associated with which group, and designate a number for each group. The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group is assigned as Group 0.
2. The GROUP system variable can only be set either at each individual telephone or when a telephone with Software Release 1.5 or greater is registered to an Avaya Communication Manager (CM) server with CM Release 4.0 or greater. In the former case, the GROUP Craft (local administrative) procedure must be invoked as specified in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*. In the latter case, GROUP is administrable on a phone-by-phone basis on the CM Station Form.
3. Once the GROUP assignments are in place, edit the configuration file to allow each telephone of the appropriate group to download its proper settings.

Here is an example of the configuration file for the Call Center agent:

```
IF $GROUP SEQ 1 goto CALLCENTER
IF $GROUP SEQ 2 goto HOTDESK
{specify settings unique to Group 0}
goto END

# CALLCENTER
{specify settings unique to Group 1}
goto END

# HOTDESK
{specify settings unique to Group 2}

# END
{specify settings common to all Groups}
```

Chapter 7: Administering Telephone Options

Administering Options for the 9600 Series IP Telephones

This chapter explains how to change parameters by means of the DHCP or HTTP servers. In all cases, you are setting a system parameter in the telephone to a desired value. Table 11 lists:

- the parameter names,
- their default values,
- the valid ranges for those values, and
- a description of each one.

For DHCP, the DHCP Option sets these parameters to the desired values as discussed in DHCP and File Servers on page 55. For HTTP, the parameters in Table 11 are set to desired values in the script file. For more information, see Contents of the Settings File on page 82. When using a media server, see Table 11: 9600 Series IP Telephone Customizable System Parameters on page 86 for information on parameters set by the file server application.

Avaya recommends that you administer options on the 9600 Series IP Telephones using script files. Some DHCP applications have limits on the amount of user-specified information. The administration required can exceed those limits for the more full-featured telephone models.

You might choose to completely disable the capability to enter or change option settings from the dialpad. You can set the system value, PROCPSWD, as part of standard DHCP/HTTP administration. Alternately, you can set PROCPSWD on the system-parameters ip-options form, as of Communication Manager Release 4.0. If PROCPSWD is non-null and consists of 1 to 7 digits, a user cannot invoke any local options without first entering the PROCPSWD value on the Craft Access Code Entry screen. For more information on craft options, see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

CAUTION:

If you administer PROCPSWD as part of DHCP/HTTP administration, the value is stored and transmitted unencrypted. Therefore, do not consider PROCPSWD as a high-security technique to inhibit a sophisticated user from obtaining access to local procedures unless you administer it using page 3 of the system-parameters IP-options form, as of Avaya Communication Manager Release 4.0.

Administering this password limits access to all local procedures, including VIEW. VIEW is a read-only Craft option that allows review of the current telephone settings.

Note:

All system parameters related to Virtual Private Network (VPN) setup and maintenance are described in the *VPN Setup Guide for 9600 Series IP Telephones* (Document # 16-602968).

Table 11: 9600 Series IP Telephone Customizable System Parameters

Parameter Name	Default Value	Description and Value Range
AGCHAND	1	Automatic Gain Control status for handset (0=disabled, 1=enabled).
AGCHEAD	1	Automatic Gain Control status for headset (0=disabled, 1=enabled).
AGCSPKR	1	Automatic Gain Control status for Speaker (0=disabled, 1=enabled).
AMADMIN	" " (Null)	WML-Application URI. The URI used to obtain the AvayaMenuAdmin.txt file for WML-applications under the A (AVAYA) Menu. Specify the HTTP server and directory path to the administration file. Do not specify the administration file name. For more information, see Avaya "A" Menu Administration on page 146.
APPNAME	" " (Null)	Primary application image file name, as provided in the 9600upgrade.txt file.
APPSTAT	1	Controls whether specific applications are enabled, restricted, or disabled. Values are: 1=all applications enabled, 2=Speed Dial (Contacts) changes and Call Log disabled and Redial last number only, 3=Speed Dial (Contacts) changes disabled, 0=Speed Dial (Contacts) changes, Call Log, and Redial disabled.

1 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
AUDASYS	3	Globally controls audible alerting. Possible system settings for audible alerting are "0" through "3" as follows: 0=Audible Alerting is Off; user cannot change this setting. 1=Audible Alerting is On; user cannot change this setting. 2=Audible Alerting is Off; user can change this setting. 3=Audible Alerting is On; user can change this setting.
AUDIOENV	0	Audio environment selection index. Valid values are 0 through 299. Note that pre-Release 2.0 software has different valid ranges.
AUDIOSTHD	0	Headset sidetone setting. Valid values for applicable sidetone masking ratings (STMR) are: 0=16db STMR; no change to sidetone level 1=24dB STMR; three steps softer than nominal 2=36dB STMR (off); no sidetone (infinite loss, i.e., inaudible). 3=19dB STMR; one level softer than nominal 4=21dB STMR; two steps softer than nominal 5=27dB STMR; four steps softer than nominal 6=30dB STMR; five steps softer than nominal 7=33dB STMR; six steps softer than nominal 8=13dB STMR; one step louder than nominal 9=10dB STMR; two steps louder than nominal Pre-Release 2.0 software has different valid ranges.
AUDIOSTHS	0	Handset sidetone setting. Valid values are: 0=16db STMR; no change to sidetone level 1=24dB STMR; three steps softer than nominal 2=36dB STMR (off); no sidetone (infinite loss, i.e., inaudible). 3=19dB STMR; one level softer than nominal 4=21dB STMR; two steps softer than nominal 5=27dB STMR; four steps softer than nominal 6=30dB STMR; five steps softer than nominal 7=33dB STMR; six steps softer than nominal 8=13dB STMR; one step louder than nominal 9=10dB STMR; two steps louder than nominal Pre-Release 2.0 software has different valid ranges.
AUTH	0	Script file authentication value (0=HTTP is acceptable, 1=HTTPS is required).
BAKLIGHTOFF	120	Number of minutes without display activity to wait before turning off the backlight. The default is 120 minutes (2 hours). Valid values range from zero (never turn off) to 999 minutes (16.65 hours).

2 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
BRAUTH	0	Backup/restore authentication control. Valid values are: 1=If at least one digital certificate has been downloaded based on TRUSTCERTS, the IP address of the call server with which the telephone is registered and the telephone's registration password will be included as the credentials in an Authorization request-header in each transmitted GET and PUT method if and only if the value of BRAUTH is "1". 0=telephone's call server IP Address and registration password is not included as part of GET or PUT Authorization header, or no digital certificate has been downloaded.
BRURI	" " (Null)	URL used for backup and retrieval of user data. Specify HTTP or HTTPS server and directory path and/or port number to backup file. Do not specify backup file name. Value: 0-255 ASCII characters. Null is a valid value and spaces are allowed. A subdirectory can be specified, for example: **SET BRURI http://135.8.60.10/backup** This puts the user backup/restore files in a subdirectory away from all other files (.bins, .txts, etc.) and permits authentication to be turned on for that subdirectory, without turning it on for the root directory.
CLDELCALLBK	0	Call Log Delete Callback Flag. Deletes calls from the Missed Call Log when the user returns the call from the Call Log. Values are 1=No, 0=Yes.
CNAPORT	50002	Avaya Converged Network Analyzer (CNA) server registration transport-layer port number (0-65535).
CNASRVR	" " (Null)	Text string containing the IP Addresses of one or more Avaya Converged Network Analyzer (CNA) servers to be used for registration. Format is dotted decimal or DNS format, separated by commas, with no spaces Zero to 255 ASCII characters, including commas.
DHCPSRVR	" " (Null)	Specifies DHCP server address(es). Format is dotted decimal or DNS format, separated by commas, with no spaces. Zero to 255 ACSII characters, including commas.
DHCPSTD	0	DHCP Standard lease violation flag. Indicates whether to keep the IP Address if there is no response to lease renewal. If set to "1" (No) the telephone strictly follows the DHCP standard with respect to giving up IP Addresses when the DHCP lease expires. If set to "0" (Yes) the telephone continues using the IP Address until it detects reset or a conflict (see DHCP Generic Setup on page 58).

3 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DIALFEATURES	" " (Null)	A list of feature number identifiers for softkey features potentially available in the Dialing call state, for example, Redial. Zero to 255 ASCII characters consisting of zero to five whole numbers separated by commas without any intervening spaces. For more information, see Administering Features on Softkeys on page 117.
DNSSRVR	0.0.0.0	Text string containing the IP Address of zero or more DNS servers, in dotted-decimal format, separated by commas with no intervening spaces (0-255 ASCII characters, including commas).
DOMAIN	" " (Null)	Text string containing the domain name to be used when DNS names in system values are resolved into IP Addresses. Valid values are 0-255 ASCII characters. If Null, no spaces allowed.
DOT1X	0	802.1X Supplicant operation mode. Valid values are: 0=With PAE pass-through, 1=with PAE pass-through and proxy Logoff, 2=without PAE pass-through or proxy Logoff. For more information, see IEEE 802.1X on page 104.
DOT1XSTAT	0	Determines how the telephone handles Supplicants. Valid values are: 0=Supplicant operation is completely disabled. 1=Supplicant operation is enabled, but responds only to received unicast EAPOL messages. 2= Supplicant operation is enabled and responds to received unicast and multicast EAPOL messages. For more information, see IEEE 802.1X on page 104.
DROPCLEAR	1	VPN only. Specifies the treatment of clear IPsec packets. One ASCII numeric digit. Valid values are: 0= all other packets will be processed, but not by IPsec, or 1=all other packets will be discarded.
ENHDIALSTAT	1	Enhanced Dialing Status. If set to “1” the Dialing Methods feature is turned on for all associated applications. If set to “0” the feature is turned off.
FBONCASCREEN	0	For the 9630/9630G/9640/9640G IP Telephones, indicates whether to display feature buttons on available lines on the Call Appearance (Phone) screen. Values are: 1=Yes; 0=No.
GRATARP	0	Gratuitous ARP flag. Controls whether the telephone will process gratuitous ARPS or ignore them. Valid values are: 1 = Yes, process gratuitous ARPS 0 = No, ignore gratuitous ARPS
GUESTDURATION	2	Guest login duration in hours. One or two ASCII numeric digits. Valid values are "1" through "12".

4 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
GUESTLOGINSTAT	0	Guest login permission flag. If "1" the Guest Login option is listed on the Avaya Menu; if "0" the Guest Login option is not available.
GUESTWARNING	5	Guest login warning in minutes to indicate when to notify the user that GUESTLOGINDURATION will expire. One or two ASCII numeric digits. Valid values are "1" through "15".
HEADSYS	1	Headset operational mode. One ASCII numeric digit. Valid values are: 0 or 2 =General Operation, where a disconnect message returns the telephone to an idle state. 1 or 3 = Call Center Operation, where a disconnect message does not change the state of the telephone.
HOMEIDLETIME	10	For 9670G IP Telephones only, the number of minutes after which the Home screen will be displayed.Value is 1 or 2 ASCII numeric digits, "5" through "30". If you prefer an idle Web page to display instead of the Home screen, set this value to less than the WMLIDLETIME value.
HTTPDIR	" " (Null)	HTTP server directory path. The path name prepended to all file names used in HTTP and HTTPS get operations during initialization. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required. The command syntax is “SET HTTPDIR *myhttpdir*” where “myhttpdir” is your HTTP server path. HTTPDIR is the path for all HTTP operations **except** for BRURI.
HTTPPORT	80	TCP port number used for HTTP file downloading. 2 to 5 ASCII numeric digits. Valid values are “80” through “65535”. Note that when the file server is on Communication Manager, set this value to “81” (port required for HTTP downloads) rather than the using the default.
HTTPSRVR	" " (Null)	IP Address(es) or DNS Name(s) of HTTP file servers used to download telephone files. Dotted decimal or DNS format, separated by commas (0-255 ASCII characters, including commas).
ICMPDU	0	Controls whether ICMP Destination Unreachable messages will be processed. Values are: 0=No, 1=Send limited Port Unreachable messages, 2=Send Protocol and Port Unreachable messages.
ICMPRED	0	Controls whether ICMP Redirect messages will be processed. Values are: 0=No, 1=Yes.
IDLEFEATURES	" " (Null)	A list of feature number identifiers for softkey features potentially available in the Idle call state, for example, Redial. Zero to 255 ASCII characters consisting of zero to six whole numbers separated by commas without any intervening spaces. For more information, see Administering Features on Softkeys on page 117.

5 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
L2Q	0	Controls whether Layer 2 frames have IEEE 802.1Q tags (0=auto, 1=enabled, 2=disabled).
L2QVLAN	0	802.1Q VLAN Identifier (0 to 4094). Null (" ") is not a valid value and the value cannot contain spaces. VLAN identifier used by IP telephones. Set this parameter only when IP telephones are to use a VLAN that is separate from the default data VLAN. If the VLAN identifier is to be configured via H.323 signaling based on Avaya Communication Manager administration forms, it should not be set here. As of software Release 2.0, L2QVLAN will always be initialized from the corresponding system initialization value at power-up, but will not be initialized from the system initialization value after a reset.
LANG0STAT	1	Controls whether the built-in English language text strings can be selected by the user. Valid values are: 0 = User cannot select English language text strings 1 = User can select English language text strings. SET LANG0STAT 1
LANGxFILE	" " (Null)	Contains the name of the language file *x*, where *x* is 1 through 4. The file name must end in .txt. Example: SET LANG1FILE “mlf_russian.txt” LANG1FILE = LANG2FILE = LANG3FILE = LANG4FILE =
LANGLARGEFONT	" " (Null)	Larger text font file name. A string of up to 32 characters specifies the loadable language file on the HTTP server for the Large Text font.
LANGSYS	" " (Null)	System-wide language that contains the name of the default system language file, if any. Value is 0 to 32 ASCII characters. The file name must end in .txt. The default is a null string. Example: SET LANGSYS “mlf_german.txt”
LOGBACKUP	1	Indicates whether the user’s Call Log should be backed up. Values are: 1=Yes; the Call Log is backed up to the same backup file as all other user data (see Table 16 for information), subject to normal administration of that file. 0=No.
LOGLOCAL	0	Event Log Severity Level (one 0-8 ASCII numeric digit). Controls the level of events logged in the endptRecentLog and endptResetLog objects in the SNMP MIB. Events with the selected level and with a higher severity level will be logged. Valid values are: 0=Disabled, 1=emergencies, 2=alerts, 3=critical, 4=errors, 5=warnings, 6=notices, 7=information, 8=debug.

6 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
LOGMISSEDONCE	0	Indicates that only one Call Log entry for multiple Missed calls from the same originating phone number should be maintained. Values are: 1=Yes; each Missed Call Log entry is maintained, along with a Missed Call counter that tracks the number of times (up to 99) the originating number called. 0=No; each Missed Call creates a new Call Log entry.
LOGSRVR	" " (Null)	Voice Monitoring Manager (VMM) Server Address. Zero or one IP Address in dotted-decimal format or DNS Name format (0-15 ASCII characters).
LOGUNSEEN	0	Indicates that a Call Log entry should be maintained for calls that are redirected from the telephone, for example, Call forwarded calls. Values are: 1=Yes; 0=No. **Note:** CM 5.2 or later is required for this feature to work.
MCIPADD	0.0.0.0	Call Server Address. Zero or more Avaya Communication Manager server IP Addresses. Format is dotted-decimal or DNS name format, separated by commas without intervening spaces (0-255 ASCII characters, including commas). Null is a valid value.
MSGNUM	" " (Null)	Voice mail system telephone/extension number. Specifies the number to be dialed automatically when the telephone user presses the **Message** button. MSGNUM is only used when the phone is aliased using non-native support. Messaging must be configured for native support. Value: 0-30 ASCII dialable characters (0-9, * and #) and no spaces. Null is a valid value.
MYCERTCAID	"CAIdentifier"	Certificate Authority Identifier to be used in a certificate request. 0 to 255 ASCII characters.
MYCERTCN	"$SERIALNO"	Common Name of the Subject of a certificate request. 0 to 255 ASCII characters that contain the string "$SERIALNO" or "$MACADDR".
MYCERTDN	" " (Null)	Additional information for the Subject of a certificate request. 0 to 255 ASCII characters
MYCERTKEYLEN	1024	Bit length of the private key to be generated for a certificate request. 4 ASCII numeric digits, "1024" through "2048".
MYCERTRENEW	90	Percentage of a certificate's Validity interval after which renewal procedures will be initiated. 1 or 2 ASCII numeric digits, "1" through "99".
MYCERTURL	" " (Null)	URL to be used to contact an SCEP server. 0 to 255 ASCII characters, zero or one URL.

7 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
MYCERTWAIT	1	Specifies whether the telephone will wait until a pending certificate request is complete, or whether it will periodically check in the background. 1 ASCII numeric digit, "0" or "1" as follows: 1 = If a connection to the SCEP server is successfully established, SCEP will remain in progress until the request for a certificate is granted or rejected. 0 = SCEP will remain in progress until the request for a certificate is granted or rejected or until a response is received indicating that the request is pending for manual approval.
OPSTAT	111	Options status flag(s) (1 or 3 ASCII numeric digits) indicate which options are user-selectable. The default of 111 grants access to all options and related applications. Single digit valid values are: 1=user can access all options, including Logout, 2= user can access only view-oriented applications. Three-digit valid values are a concatenation of binary values, in the form *abc*, where each letter represents a 0 (disabled/off) or 1 (enabled/on), interpreted as: *a* = base settings for all user options and related applications, except as noted in *b* or *c*. *b* = setting for view-oriented applications (for example, the Network Information application), as applicable. *c* = setting for Logout application, if applicable. The binary "0" does not allow an end user to see or invoke options and related applications. The binary "1" allows full display and access to all options and related applications.
OPSTAT2	0	OPSTAT override flag. If set to 0, OPSTAT is not affected. If set to 1, OPSTAT is unaffected with the exception that any changes to customized labels in the backup file are uploaded and used as if OPSTAT permitted this action.
NVHTTPSRVR	0.0.0.0	VPN and non-VPN. HTTP file server IP addresses used to initialize HTTPSRVR the next time the phone starts up. 0 to 255 ASCII characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. As of Software Release 3.1, NVHTTPSRVR is provided for VPN mode so that a file server IP address can be preconfigured and saved in non-volatile memory. See the *VPN Setup Guide for 9600 Series IP Telephones* (Document # 16-602968) for VPN use.

8 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
NVTLSSRVR	0.0.0.0	VPN and non-VPN. HTTPS file server IP addresses used to initialize TLSSRVR the next time the phone starts up. 0 to 255 ASCII characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. For VPN use, see the *VPN Setup Guide for 9600 Series IP Telephones* (Document # 16-602968).
PHNCC	1	Telephone country code. The administered international country code for the location by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1-3 digits, from “1” to “999.”
PHNDPLENGTH	5	Internal extension telephone number length. Specifies the number of digits associated with internal extension numbers by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from “3” to “13.”
PHNEMERGNUM	" " (Null)	Emergency telephone/extension number. Specifies the number to be dialed automatically when the telephone user presses the **Emerg** button. Value: 0-30 ASCII dialable characters (0-9, * and #) and no spaces. Null is a valid value.
PHNIC	011	Telephone international access code. The maximum number of digits, if any, dialed to access public network international trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-4 digits.
PHNLD	1	Telephone long distance access code. The digit, if any, dialed to access public network long distance trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 digit or " " (Null).
PHNLDLENGTH	10	Length of national telephone number. The number of digits in the longest possible national telephone number by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from “3” to “10.” Range: 1 or 2 ASCII numeric characters, from “5” to “15.”
PHNOL	9	Outside line access code. The character(s) dialed, including # and *, if any, to access public network local trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-2 dialable characters, including " " (Null).
PHY1STAT	1	Ethernet line interface setting (1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex, and 6=1000Mbps full-duplex if supported by the hardware).

9 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PHY2PRIO	0	Layer 2 priority value for frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is "1" (enabled). Values are from 0-7 and correspond to the drop-down menu selection.
PHY2STAT	1	Secondary Ethernet interface setting (0=Secondary Ethernet interface off/disabled, 1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex), and 6=1000Mbps full-duplex if supported by the hardware).
PHY2VLAN	0	VLAN identifier used by frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is “1” (enabled). Value is 1-4 ASCII numeric digits from “0” to “4094.” Null is not a valid value, nor can the value contain spaces. If this value is set by LLDP using the Port VLAN ID TLV value, it will not change regardless of settings from other sources. For more information, see Parameter Data Precedence.
PROCPSWD	27238	Text string containing the local (dialpad) procedure password (Null or 1-7 ASCII digits). If set, password must be entered immediately after accessing the Craft Access Code Entry screen, either during initialization or when Mute (or Contacts for the 9610) is pressed to access a craft procedure. Intended to facilitate restricted access to local procedures even when command sequences are known. Password is viewable, not hidden.
PROCSTAT	0	Local (dialpad) Administrative Options status (0=all Administrative (Craft) Options are allowed, 1=only VIEW is allowed).
PUSHCAP	2222	Push capabilities. Valid values are any three or four digit combination using only the digits "0", "1", or "2". For information on push messaging and administration, see the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-600888).
PUSHPORT	80	TCP listening port number used for the telephone’s HTTP server. 2 to 5 ASCII numeric digits, "80" through "65535".

QKLOGINSTAT	1	Quick login permission flag. Valid values are:
		1= Quick login permitted; user must press the # key to see the previous Extension and Password.
		0= Quick login not permitted; the user must explicitly enter the Extension and Password.

10 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
QTESTRESPONDER	" " (Null)	Specifies the IP Address to which Qtest messages should be sent. Format is dotted decimal or DNS format, separated by commas, with no spaces. Zero to 255 ASCII characters, including commas.
REREGISTER	20	Registration timer in minutes. Controls an H.323 protocol timer that should only be changed under very special circumstances by someone who fully understands the system operation impact. Value is 1-120.
RINGBKFEATURES	" " (Null)	A list of feature number identifiers for softkey features potentially available in the active (with far end ringback) call state. Zero to 255 ASCII characters consisting of zero to three whole numbers separated by commas without any intervening spaces. For more information, see Administering Features on Softkeys on page 117.
RINGTONESTYLE	0	The Ring Tone Style Menu initially offered to the user (0=Classic; 1=Alternate, more modern ringtones).
RTCPMON	" " (Null)	Text string containing the 4-octet IP Address of the RTCP monitor currently in use, in dotted decimal or DNS Name format (0-15 ASCII characters, no spaces).
SCEPPASSWORD	"$SERIALNO"	Specifies a challenge password for SCEP. Zero .to 32 ASCII characters
SCREENSAVER	" " (Null)	Filename for a custom screen saver. 0 to 32 ASCII characters. System value initialization checks this parameter for a value during telephone startup. Note that screen saver files must be in .jpg format. Acceptable characters for use in filenames are: 0 through 9 A through Z a through z - (dash) . (period) _ (underscore)
SCREENSAVERON	240	Number of idle time minutes after which the screen saver is turned on. The default is 240 minutes (4 hours). Valid values range from zero (disabled) to 999 minutes (16.65 hours). For 9670G phones, use HOMEIDLETIME instead.
SNMPADD	" " (Null)	Text string containing zero or more allowable source IP Addresses for SNMP queries, in dotted decimal or DNS format, separated by commas, with up to 255 total ASCII characters including commas. Note that as of Avaya Communication Manager Release 4.0, SNMP addresses can also be administered on the system-parameters IP-options form.

11 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
SNMPSTRING	" " (Null)	Text string containing the SNMP community name string (up to 32 ASCII characters, no spaces). Note that as of Avaya Communication Manager Release 4.0, the SNMP community string can also be administered on the system-parameters IP-options form.
STATIC	0	Static programming override flag. If set to “0” static programming never overrides call server (DHCP) or call server administered data. If set to “1” static programming overrides only file server administered data. If set to “2” static programming overrides only call server administered data. If set to “3” static programming overrides both file server- and call server-administered data. Allows a call server IP Address that has been manually programmed into a telephone to override any value received via DHCP or via this configuration file. A manually programmed IP Address will only be used if it is not 0.0.0.0, so this parameter may be used to allow only specific telephones to use a different value than otherwise provided by this configuration file. If STATIC is to be used to select a manual override of file server IP Address(es), STATIC must be set via DHCP, not via this configuration file.
SUBSCRIBELIST	" " (Null)	One or more Push application server subscription URLs, separated by commas without any intervening spaces (0-255 ASCII characters, including commas).
TALKFEATURES	" " (Null)	A list of feature number identifiers for softkey features potentially available for the entire active call state. Zero to 255 ASCII characters consisting of zero to three whole numbers separated by commas without any intervening spaces. For more information, see Administering Features on Softkeys on page 117.
TLSDIR	" " (Null)	Path name prepended to all file names used in HTTP GET operations during startup. Zero to 127 ASCII characters.
TLSPORT	411	TCP port number used for HTTP file downloading. 2 to 5 ASCII numeric digits. Valid values are "80" through "65535".
TLSSRVRID	1	Controls whether the identity of a TLS server is checked against its certificate. 1 ASCII numeric digit. Valid values are: 1=Provides additional security by checking to verify that the server certificate’s DNS name matches the DNS name used to contact the server. 0=Certificate is not checked against the DNS name used to contact the server.

12 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
TPSLIST	" " (Null)	One or more trusted domain/path strings, separated by commas without any intervening spaces (0-255 ASCII characters, including commas). A URL pushed to a telephone must contain one of these strings if it is to be used to obtain content to be rendered by the telephone.
TRUSTCERTS	" " (Null)	File names of third-party trusted certificates to be downloaded. Zero or more file names or URLs, separated by commas without any intervening spaces; must be in PEM format.
UNNAMEDSTAT	1	Unnamed Registration Status. Specifies whether unnamed registration is initiated if the user fails to enter a value at the `Extension:` prompt or Login screen. Unnamed registration provides the telephone with a TTI-level service, enabling a user, for example, to dial emergency services like 911. Value 1=Yes, 0=No.
USBLOGINSTAT	1	USB Login Permission Flag, specifying if the user is allowed to log in to the call server via a USB Login profile. Valid values are: 1=Yes 2=No
USBPOWER	2	Determines for which telephone powering arrangements power will be provided to the telephone's USB interface (all models except 9610). 1 ASCII numeric digit. Valid values are: 0=Turn off USB power regardless of power source. 1=Turn on USB power only if using auxiliary power. 2=Turn on USB power regardless of power source. 3=Turn on USB power if Aux powered or PoE Class 3 power.
VLANSEP	1	VLAN separation. Controls whether frames to/from the secondary Ethernet interface receive IEEE 802.1Q tagging treatment. The tagging treatment enables frames to be forwarded based on their tags in a manner separate from telephone frames. If tags are not changed, no tag-based forwarding is employed. Values are: 1=On/Enabled, 2= Off/Disabled. This parameter is used with several related parameters. For more information, see VLAN Separation on page 102.
VLANTEST	60	Number of seconds to wait for a DHCPOFFER when using a non-zero VLAN ID (1-3 ASCII digits, from "0" to "999").
VOXFILES	" " (Null)	A list of voice language file names, used in the voice-initiated dialing process. 0 to 255 ASCII characters; zero or more file names separated by commas without any intervening spaces. See Administering Voice-Initiated Dialing on page 113 for more information.

13 of 14

Table 11: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
WEATHERAPP	"default"	The URL from which to request weather information. Zero to 255 ASCII characters: zero or one URL or the word "default".
WMLEXCEPT	" " (Null)	One or more HTTP proxy server exception domains that do not require the use of the proxy server (0-127 ASCII characters, including commas, without any intervening spaces). Set this parameter only if a proxy server is used and if there are exception domains.
WMLHOME	" " (Null)	URL that specifies the home page for Web browsers that use WML, except the 9610. Zero or one URL (0-255 ASCII characters, including spaces, if any). If Null, the Web application will not be displayed.
WMLIDLETIME	10	Idle time before displaying Web page. The number of minutes of inactivity after which the Web browser will be displayed if WMLIDLEURI is not null. The default is 10 minutes. Valid values range from 1 to 999 minutes (16.65 hours).
WMLIDLEURI	" " (Null)	Idle time Web page URI. URI that specifies the Web page the browser displays after an idle interval. Value: Zero or one URI (0-255 ASCII characters, no spaces). Null is valid but if Null, no page displays. Avaya recommends that WMLIDLEURI be specified for telephones in public areas through the use of a GROUP parameter. The idle timer is only reset if WMLIDLEURI is non-null such that an HTTP GET can be sent.
WMLPORT	8000	TCP port number for the HTTP proxy server, if applicable (1-5 ASCII numeric characters from “0” to “65535.” Null is not a valid value.
WMLPROXY	" " (Null)	One HTTP proxy server IP Address in dotted decimal or DNS Name format (0-255 ASCII characters). Set this parameter only if Web pages requiring a proxy server will be supported or if the 9670G Weather and/or World Clock applications will be used.
WMLSMALL		Idle screen for the 9610 WML browser (only). Zero (0) to 255 ASCII characters. Zero or one URL. Other 9600 Series telephones use WMLHOME instead.
WORLDCLOCKAPP	"default"	The URL from which to request time information. Zero to 255 ASCII characters: zero or one URL or the word "default".

14 of 14

Note:

Table 11 applies to all 9600 Series IP Telephones. Certain 9600 IP Telephones might have additional, optional information that you can administer. For more information, see Chapter 8: Administering Applications and Options.

VLAN Considerations

This section contains information on how to administer 9600 Series IP Telephones to minimize registration time and maximize performance in a Virtual LAN (VLAN) environment. If your LAN environment does not include VLANs, set the system parameter L2Q to 2 (off) to ensure correct operation.

VLAN Tagging

IEEE 802.1Q tagging (VLAN) is a useful method of managing VoIP traffic in your LAN. Avaya recommends that you establish a *voice* VLAN, set L2QVLAN to that VLAN, and provide voice traffic with priority over other traffic. If LLDP was used set the telephones' VLAN, that setting has absolute authority. Otherwise, you can set VLAN tagging manually, by DHCP, or in the 46xxsettings.txt file.

If VLAN tagging is enabled (L2Q=0 or 1), the 9600 Series IP Telephones set the VLAN ID to L2QVLAN, and VLAN priority for packets from the telephone to L2QAUD for audio packets and L2QSIG for signalling packets. The default value (6) for these parameters is the recommended value for voice traffic in IEEE 802.1D.

Regardless of the tagging setting, a 9600 Series IP Telephone will always transmit packets from the telephone at absolute priority over packets from secondary Ethernet. The priority settings are useful only if the downstream equipment is administered to give the *voice* VLAN priority.

VLAN Detection

The Avaya IP Telephones support automatic detection of the condition where the L2QVLAN setting is incorrect. When VLAN tagging is enabled (L2Q= 0 or 1) initially the 9600 Series IP Telephone transmits DHCP messages with IEEE 802.1Q tagging and the VLAN set to L2QVLAN. The telephones will continue to do this for VLANTEST seconds.

- If the VLANTEST timer expires and L2Q=1, the telephone sets L2QVLAN=0 and transmits DHCP messages with the default VLAN (0).
- If the VLANTEST timer expires and L2Q=0, the telephone sets L2QVLAN=0 and transmits DHCP messages without tagging.
- If VLANTEST is 0, the timer will never expire.

  Note:

  Regardless of the setting of L2Q, VLANTEST, or L2QVLAN, you must have DHCP administered so that the telephone will get a response to a DHCPDISCOVER when it makes that request on the default (0) VLAN.

  After VLANTEST expires, if an Avaya IP Telephone running R1.2 receives a non-zero L2QVLAN value, the telephone will release the IP Address and send DHCPDISCOVER on that VLAN. Any other release will require a manual reset before

the telephone will attempt to use a VLAN on which VLANTEST has expired. See the Reset procedure in Chapter 3 of the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*.

The telephone ignores any VLAN ID administered on the call server if a non-zero VLAN ID is administered either:

- by LLDP,
- manually,
- through DHCP, and/or
- in the settings file.

VLAN Default Value and Priority Tagging

The system value **L2QVLAN** is initially set to “0” and identifies the 802.1Q VLAN Identifier. This default value indicates “priority tagging” as defined in IEEE 802.IQ Section 9.3.2.3. Priority tagging specifies that your network closet Ethernet switch automatically insert the switch port default VLAN without changing the user priority of the frame (cf. IEEE 802.1D and 802.1Q).

The VLAN ID = 0 (zero) is used to associate priority-tagged frames to the port/native VLAN of the ingress port of the switch. But some switches do not understand a VLAN ID of zero and require frames tagged with a non-zero VLAN ID.

If you do not want the default VLAN to be used for voice traffic:

- Ensure that the switch configuration lets frames tagged by the 9600 Series IP Telephone through without overwriting or removing them.
- Set the system value **L2QVLAN** to the ***VLAN ID*** appropriate for your voice LAN.

Another system value you can administer is **VLANTEST**. VLANTEST defines the number of seconds the 9600 IP Series Telephone waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is “60” seconds. Using VLANTEST ensures that the telephone returns to the default VLAN if an invalid VLAN ID is administered or if the phone moves to a port where the L2QVLAN value is invalid. The default value is long, allowing for the scenario that a major power interruption is causing the phones to restart. Always allow time for network routers, the DHCP servers, etc. to be returned to service. If the telephone restarts for any reason and the VLANTEST time limit expires, the telephone assumes the administered VLAN ID is invalid. The telephone then initiates registration with the default VLAN ID.

Setting **VLANTEST** to “**0**” has the special meaning of telling the phone to use a non-zero VLAN indefinitely to attempt DHCP. In other words, the telephone does not return to the default VLAN.

Note:

If the telephone returns to the default VLAN but must be put back on the L2QVLAN VLAN ID, you must Reset the telephone. See the Reset procedure in the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*.

VLAN Separation

VLAN separation is available to control priority tagging from the device on the secondary Ethernet, typically PC data. The following system parameters control VLAN separation:

- **VLANSEP** - enables (1) or disables (0) VLAN separation.
- **PHY2VLAN** - provides the VLAN ID for tagged frames received on the secondary Ethernet interface.
- **PHY2PRIO** - the layer 2 priority value to be used for tagged frames received on the secondary Ethernet interface.

Table 12 provides several VLAN separation guidelines.

Note:

The 9610 IP Telephone does not support full VLAN separation because it has no secondary Ethernet interface and therefore never has PHY2VLAN and PHY2PRIO values.

Table 12: VLAN Separation Rules

If		Then
VLANSEP is “0”,	**OR** the telephone is not tagging frames, **OR** the telephone is tagging frames with a VLAN ID equal to PHY2VLAN.	Frames received on the secondary Ethernet interface will not be changed before forwarding. For example, tagging is not added or removed and the VLAN ID and tagged frames priority are not changed. The Ethernet switch forwarding logic determines that frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the telephone without regard to specific VLAN IDs or the existence of tags.
VLANSEP is “1” (On/Enabled)		All tagged frames received on the secondary Ethernet interface are changed before forwarding to make the VLAN ID equal to the PHY2VLAN value and the priority value equal to the PHY2PRIO value. Untagged frames received on the secondary Ethernet interface are not changed before forwarding. Tagged frames with a VLAN ID of zero (priority-tagged frames) will either be: - forwarded without being changed (preferred), or - changed before they are forwarded such that the VLAN ID of the forwarded frame is equal to the PHY2VLAN value and the priority value is equal to the PHY2PRIO value.

1 of 2

Table 12: VLAN Separation Rules (continued)

If		Then
VLANSEP is “1” (On/Enabled)	**AND** the telephone is not tagging frames, **OR** if the telephone is tagging frames with a VLAN ID equal to PHY2VLAN, **OR** if the PHY2VLAN value is zero.	The Ethernet switch forwarding logic determines that frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the telephone without regard to specific VLAN IDs or the existence of tags. Frames received on the secondary Ethernet interface will not be changed before forwarding. In other words, tagging is not added or removed, and the VLAN ID and priority of tagged frames is not changed.
VLANSEP is “1” (On/Enabled)	**AND** the telephone is tagging frames with a VLAN ID not equal to PHY2VLAN, **AND** the PHY2VLAN value is not zero.	Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2VLAN. Tagged frames received on the Ethernet line interface will only be forwarded to the telephone if the VLAN ID equals the VLAN ID used by the telephone. Untagged frames will continue to be forwarded or not forwarded as determined by the Ethernet switch forwarding logic. Tagged frames with a VLAN ID of zero (priority-tagged frames) will either be: - forwarded to the secondary Ethernet interface or the telephone as determined by the forwarding logic of the Ethernet switch (preferred), or - dropped.

DNS Addressing

The 9600 IP Telephones support DNS addresses and dotted decimal addresses. The telephone attempts to resolve a non-ASCII-encoded dotted decimal IP Address by checking the contents of DHCP Option 6. See DHCP Generic Setup on page 58 for information. At least one address in Option 6 must be a valid, non-zero, dotted decimal address, otherwise, DNS fails. The text string for the **DOMAIN** system parameter (Option 15, Table 11) is appended to the address(es) in Option 6 before the telephone attempts DNS address resolution. If Option 6 contains a list of DNS addresses, those addresses are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS by DHCP, you can specify the DNS server and/or Domain name in the HTTP script file. But first **SET** the **DNSSRVR** and **DOMAIN** values so you can use those names later in the script.

Note:

Administer Options 6 and 15 appropriately with DNS servers and Domain names respectively.

IEEE 802.1X

Except for the 9610, 9600 Series IP Telephones support the IEEE 802.1X standard for pass-through and Supplicant operation. The system parameter DOT1X determines how the telephones handle 802.1X multicast packets and proxy logoff, as follows:

- When DOT1X = 0, the telephone forwards 802.1X multicast packets from the Authenticator to the PC attached to the telephone and forwards multicast packets from the attached PC to the Authenticator (multicast pass-through). Proxy Logoff is not supported. This is the default value.
- When DOT1X = 1, the telephone supports the same multicast pass-through as when DOT1X=0. Proxy Logoff is supported.
- When DOT1X = 2, the telephone forwards multicast packets from the Authenticator only to the telephone, ignoring multicast packets from the attached PC (no multicast pass-through). Proxy Logoff is not supported.
- Regardless of the DOT1X setting, the telephone always properly directs unicast packets from the Authenticator to the telephone or its attached PC, as dictated by the MAC address in the packet.

All 96xx telephones support Supplicant operation and parameter values as specified in IEEE 802.1X, but, as of software Release 2.0, only if the value of the parameter DOT1XSTAT is “1” or “2”. If DOT1XSTAT has any other value, Supplicant operation is not supported.

IP telephones will respond to unicast EAPOL frames (frames with the telephone’s MAC address as the destination MAC address, and a protocol type of 88-8E hex) received on the Ethernet line interface if the value of DOT1XSTAT is “1” or “2”, but will only respond to EAPOL frames that have the PAE group multicast address as the destination MAC address if the value of DOT1XSTAT is “2”. If the value of DOT1XSTAT is changed to “0” from any other value after the Supplicant has been authenticated, an EAPOL-Logoff will be transmitted before the Supplicant is disabled.

As of software Release 2.0, the system parameter DOT1XSTAT determines how the telephone handles Supplicants as follows:

- When DOT1XSTAT = 0, Supplicant operation is completely disabled. This is the default value.
- When DOT1XSTAT = 1, Supplicant operation is enabled, but responds only to received unicast EAPOL messages.
- When DOT1XSTAT = 2, Supplicant operation is enabled and responds to received unicast and multicast EAPOL messages.

Note:

If the Ethernet line interface link fails, the 802.1X Supplicant, if enabled, enters the Disconnected state. The 802.1X Supplicant variable userLogoff normally has a value of FALSE. This variable will be set to TRUE before the telephone drops the link on the Ethernet line interface (and back to FALSE after the link has been restored). The userLogoff variable may also be briefly set to TRUE to force the Supplicant into the LOGOFF state when new credentials are entered.

802.1X Pass-Through and Proxy Logoff

9600 Series IP Telephones with a secondary Ethernet interface support pass-through of 802.1X packets to and from an attached PC. This enables an attached PC running 802.1X supplicant software to be authenticated by an Ethernet data switch.

The IP Telephones support two pass-through modes:

- pass-through and
- pass-through with proxy logoff.

The DOT1X parameter setting controls the pass-through mode. In Proxy Logoff mode (DOT1X=1), when the secondary Ethernet interface loses link integrity, the telephone sends an 802.1X EAPOL-Logoff message to the data switch on behalf of the attached PC. The message alerts the switch that the device is no longer present. For example, a message would be sent when the attached PC is physically disconnected from the IP telephone. When DOT1X = 0 or 2, the Proxy Logoff function is not supported.

Note:

Because the 9610 IP Telephone does not have a secondary Ethernet interface, it does not support 802.1X pass-through or pass-through with Proxy Logoff.

802.1X Supplicant Operation

9600 IP Telephones that support Supplicant operation also support Extensible Authentication Protocol (EAP), but only with the MD5-Challenge authentication method as specified in IETF RFC 3748 [8.5-33a].

A Supplicant identity (ID) and password of no more than 12 numeric characters are stored in reprogrammable non-volatile memory. The ID and password are not overwritten by telephone software downloads. The default ID is the MAC address of the telephone, converted to ASCII format without colon separators, and the default password is null. Both the ID and password are set to defaults at manufacture. EAP-Response/Identity frames use the ID in the Type-Data field. EAP-Response/MD5-Challenge frames use the password to compute the digest for the Value field, leaving the Name field blank.

When a telephone is installed for the first time and 802.1x is in effect, the dynamic address process prompts the installer to enter the Supplicant identity and password. The IP telephone does not accept null value passwords. See “Dynamic Addressing Process” in the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*.

The IP telephone stores 802.1X credentials when successful authentication is achieved. Post-installation authentication attempts occur using the stored 802.1X credentials, without prompting the user for ID and password entry.

An IP telephone can support several different 802.1X authentication scenarios, depending on the capabilities of the Ethernet data switch to which it is connected. Some switches may authenticate only a single device per switch port. This is known as single-supplicant or port-based operation. These switches typically send multicast 802.1X packets to authenticating devices.

These switches support the following three scenarios:

- **Standalone telephone (Telephone Only Authenticates) -** When the IP telephone is configured for Supplicant Mode (DOT1XSTAT=2), the telephone can support authentication from the switch.
- **Telephone with attached PC (Telephone Only Authenticates) -** When the IP telephone is configured for Supplicant Mode (DOT1X=2 and DOT1XSTAT=2), the telephone can support authentication from the switch. The attached PC in this scenario gains access to the network without being authenticated.
- **Telephone with attached PC (PC Only Authenticates) -** When the IP telephone is configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1 and DOT1XSTAT=0), an attached PC running 802.1X supplicant software can be authenticated by the data switch. The telephone in this scenario gains access to the network without being authenticated.

Some switches support authentication of multiple devices connected through a single switch port. This is known as multi-supplicant or MAC-based operation. These switches typically send unicast 802.1X packets to authenticating devices. These switches support the following two scenarios:

- **Standalone telephone (Telephone Only Authenticates) -** When the IP telephone is configured for Supplicant Mode (DOT1XSTAT=2), the telephone can support authentication from the switch. When DOT1X is “0” or “1” the telephone is unable to authenticate with the switch.
- **Telephone and PC Dual Authentication -** Both the IP telephone and the connected PC can support 802.1X authentication from the switch. The IP telephone may be configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1 and DOT1XSTAT=1 or 2). The attached PC must be running 802.1X supplicant software.

Link Layer Discovery Protocol (LLDP)

Release 1.2 9600 Series IP Telephones support IEEE 802.1AB. Link Layer Discovery Protocol (LLDP) is an open standards layer 2 protocol IP Telephones use to advertise their identity and capabilities and to receive administration from an LLDP server. LAN equipment can use LLDP to manage power, administer VLANs, and provide some administration.

The transmission and reception of LLDP is specified in IEEE 802.1AB-2005. The 9600 Series IP Telephones use Type-Length-Value (TLV) elements specified in IEEE 802.1AB-2005, TIA

TR-41 Committee - Media Endpoint Discovery (LLDP-MED, ANSI/TIA-1057), and Proprietary elements. LLDP Data Units (LLDPDUs) are sent to the LLDP Multicast MAC address (01:80:c2:00:00:0e).

These telephones:

- do not support LLDP on the secondary Ethernet interface.
- will not forward frames received with the 802.1AB LLDP group multicast address as the destination MAC address between the Ethernet line interface and the secondary Ethernet interface.

A 9600 Series IP Telephone initiates LLDP after receiving an LLDPDU message from an appropriate system. Once initiated, the telephones send an LLDPDU every 30 seconds with the following contents:

Table 13: LLDPDU Transmitted by the 9600 Series IP Telephones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPv4 IP Address of telephone.
Basic Mandatory	Port ID	MAC address of the telephone.
Basic Mandatory	Time-To-Live	120 seconds.
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.
Basic Optional	System Capabilities	Bit 2 (Bridge) will be set in the System Capabilities if the telephone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled. Bit 5 (Telephone) will be set in the System Capabilities. If Bit 5 is set in the Enabled Capabilities than the telephone is registered.
Basic Optional	Management Address	Mgmt IPv4 IP Address of telephone. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the telephone.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports autonegotiation status and speed of the uplink port on the telephone.
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery - Class III - IP Telephone.

1 of 3

Table 13: LLDPDU Transmitted by the 9600 Series IP Telephones (continued)

Category	TLV Name (Type)	TLV Info String (Value)
TIA LLDP MED	Extended Power-Via-MDI	Power Value = 0 if the telephone is not currently powered via PoE, else the maximum power usage of the telephone plus all modules and adjuncts powered by the telephone in tenths of a watt.
TIA LLDP MED	Network Policy	Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value.
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Firmware Revision	BOOTNAME.
TIA LLDP MED	Inventory – Software Revision	APPNAME.
TIA LLDP MED	Inventory – Serial Number	Telephone serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final D***xxx*** characters removed.
Avaya Proprietary	PoE Conservation Level Support	Provides Power Conservation abilities/settings, Typical and Maximum Power values. OUI = 00-40-0D (hex), Subtype = 1.
Avaya Proprietary	Call Server IP Address	Call Server IP Address. Subtype = 3.
Avaya Proprietary	IP Phone Addresses	Phone IP Address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	CNA Server IP Address	CNA Server IP Address = in-use value from CNASRVR. Subtype = 5.
Avaya Proprietary	File Server	File Server IP Address. Subtype = 6.

2 of 3

Table 13: LLDPDU Transmitted by the 9600 Series IP Telephones (continued)

Category	TLV Name (Type)	TLV Info String (Value)
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not. Subtype = 7.
Basic Mandatory	End-of-LLDPDU	Not applicable.

3 of 3

On receipt of a LLDPDU message, the Avaya IP Telephones will act on the TLV elements described in Table 14:

Table 14: Impact of TLVs Received by 9600 Series IP Telephones on System Parameter Values

System Parameter Name	TLV Name	Impact
PHY2VLAN	IEEE 802.1 Port VLAN ID	System value changed to the Port VLAN identifier in the TLV.
L2QVLAN and L2Q	IEEE 802.1 VLAN Name	The system value is changed to the TLV VLAN Identifier. L2Q will be set to 1 (ON). VLAN Name TLV is only effective if: • The telephone is not registered with the Call Server. • Name begins with VOICE (case does not matter). • The VLAN is not zero. • DHCP Client is activated. • The telephone is registered but is not tagging layer 2 frames with a non-zero VLAN ID. If VLAN Name causes the telephone to change VLAN and the telephone already has an IP Address the telephone will release the IP Address and reset. If the TLV VLAN ID matches the VLAN ID the telephone is using, the VLAN ID is marked as set by LLDP. Otherwise, if already registered, the telephone waits until there are no active calls, releases its IP Address, turns on tagging with the TLV VLAN ID, sets L2Q to "on," changes the default L2Q to "on," and resets. If there is no valid IP Address, the telephone immediately starts tagging with the new VLAN ID without resetting.

Table 14: Impact of TLVs Received by 9600 Series IP Telephones on System Parameter Values (continued)

System Parameter Name	TLV Name	Impact
L2Q, L2QVLAN, L2QAUD, L2QSIG, DSCPAUD, DSCPSIG	MED Network Policy TLV	L2Q - set to “2” (off) If T (the Tagged Flag) is set to 0; set to “1” (on) if T is set to 1. L2QVLAN - set to the VLAN ID in the TLV. L2QAUD and L2QSIG - set to the Layer 2 Priority value in the TLV. DSCPAUD and DSCPSIG - set to the DSCP value in the TLV. A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • the value of USE_DHCP is “0” and the value of IPADD is not “0.0.0.0”, or • the Application Type is not 1 (Voice), or • the Unknown Policy Flag (U) is set to 1.
MCIPADD	Proprietary Call Server TLV	MCIPADD will be set to this value if it has not already been set.
TLSSRVR and HTTPSRVR	Proprietary File Server TLV	TLSSRVR and HTTPSRVR will be set to this value if neither of them have already been set.
L2Q	Proprietary 802.1 Q Framing	The default L2Q is set to the value of this TLV. No change is made to the current L2 tagging, but the new default value is used on the next reboot. If TLV = 1, L2Q set to "1" (On). If TLV = 2, L2Q set to "2" (Off). If TLV = 3, L2Q set to "0" (Auto).

Table 14: Impact of TLVs Received by 9600 Series IP Telephones on System Parameter Values (continued)

System Parameter Name	TLV Name	Impact
	Proprietary - PoE Conservation TLV	This proprietary TLV can initiate a power conservation mode. The telephones that support this will turn on/off the telephone backlight and the backlight of an attached Button Module in response to this TLV. Exception: the 9670G display backlight is put into low-power mode rather than being turned off.
	Extended Power-Via-MDI	Power conservation mode will be enabled if the received binary Power Source value is 10, and power conservation mode will be disabled if the received binary Power Source value is not 10. Power conservation mode is enabled even if the telephone is not powered over Ethernet because the telephone sends information about the power source that it is using in a TIA LLDP MED Extended Power-Via-MDI TLV; it is assumed that the power management system intends to conserve local power as well.

Local Administrative Options Using the Telephone Dialpad

The *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide* details how to use Craft local procedures at the telephone for administration. The local procedures you might use most often as an administrator are:

- **CLEAR** - Remove all administered values, user-specified data, option settings, etc. and return a telephone to its initial “out of the box” default values.
- **DEBUG** - Enable or disable debug mode for the button module serial port.
- **GROUP** - Set the group identifier on a per-phone basis.
- **INT** - Set or change the interface control value(s) of PHY1STAT and/or PHY2STAT.
- **RESET** - Reset the telephone to default values including any values administered through local procedures, and values previously downloaded using DHCP or a settings file.
- **RESTART** - Restart the telephone in response to an error condition, including the option to reset system values.
- **VIEW** - Review the 9600 IP Telephone system parameters to verify current values and file versions.
- **INT - Secondary Ethernet (Hub) Interface Enable/Disable** - Enable or disable the secondary Ethernet hub locally.

Language Selection

9600 Series IP Telephones are factory-set to display information in the English language. As of Release 1.1, all software downloads include language files for 13 additional languages. Software Release 1.2 added support for a large font version of English only and Release 1.5 added Arabic to the language file download. Administrators can specify from one to four languages per telephone to replace English. End users can then select which of those languages they want their telephone to display.

All downloadable language files contain all the information needed for the telephone to present the language as part of the user interface. For the 9670G IP Telephone, this includes an indication of the character to be used as a decimal "point" in numeric values and an indication of the character, if any, to be used as a separator (thousands, millions, etc.) in numeric values (no character or a space character must be usable as well as punctuation characters).

There are no dependencies between the languages available from the software download and the actual character input method. If a character input method is not supported, ASCII is used instead. Acceptable input methods are as follows:

• ASCII	• Croatian, Slovenian
• Latin-1	• Czech, Slovak
• German	• Estonian
• French	• Hungarian
• Italian	• Latvian
• Spanish	• Lithuanian
• Portuguese	• Polish
• Russian	• Romanian
• Albanian, Azeri, Turkish	

Use the configuration file and these parameters to customize the settings for up to four languages:

- **LANGxFILE** - The name of a selected language file, for example, "French". In addition to providing the language name as this value, replace the "x" in this parameter with a "1", "2", "3", or "4" to indicate which of four languages you are specifying. For example, to indicate German and French are the available languages, the setting is: **LANG1FILE=mlf_german.txt** and **LANG2FILE=mlf_french.txt**.
- **LANG0STAT** - Allows the user to select the built-in English language when other languages are downloaded. If LANG0STAT is "0" and at least one language is downloaded, the user cannot select the built-in English language. If LANG0STAT is "1" the user can select the built-in English language text strings.
- **LANGSYS** - The file name of the system default language file, if any.
- **LANGLARGEFONT** - The name of the language file you want available for a "large font" display, currently only "English."

As of Release 1.2, a large text font is available for user selection on all 9600 Series IP Telephones but the 9610. The larger text font can only be activated if a language file for this font

is available. The Text Size option is presented to the telephone user if and only if the system value LANGLARGEFONT is not null and if a language file for that value is being used as the current user interface language. If neither condition is met, the Text Size option is not presented to the user.

For example, if the language in use is English, and a large text font language file for English is specified in LANGLARGEFONT and available, the Text Size option is presented on the Screen and Sounds Options screen.

For more information, see 9600 Series IP Telephone Customizable System Parameters. To view multiple language strings, see the MLS local procedure in the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*. To download a language file or review pertinent information, go to http://support.avaya.com/unicode.

Note:

Specifying a language other than English in the configuration file has no impact on Avaya Communication Manager settings, values, or text strings.

Administering Voice-Initiated Dialing

As of software Release 2.0, all 9600 Series IP Telephones with a speakerphone microphone (all except the 9610) are capable of voice-initiated dialing.

All 96xx telephone software distribution packages include a voice language file for each of the supported languages. Administer the system parameter VOXFILES to identify the voice language file(s) you want available to your end users. All downloadable VOX language files contain data files that allow the telephone to perform the following tasks for the associated language:

- Accept a user's verbal input of keywords and Names.
- Search the local Contacts list of Names.
- Return zero, one, or more prospective matching Contacts entries.

Each voice language file has a file name beginning with three characters that indicate the language supported and ending with ".tar". The available languages and corresponding three-character filename designations are as follows:

Language	Initial Characters of the Filename
Brazilian Portuguese	PTB
European Spanish	SPE
Dutch	DUN
German	GED
Italian	ITI
Parisian French	FRF

U.K. English	ENG
U.S. English	ENU

Two voice-initiated dialing settings are available to end users by the Avaya Menu -> Call Settings option. They are Voice Dialing and Voice Dialing Language, which allow the end user to enable/disable voice-initiated dialing and select one of the voice languages you administered using the VOXFILES parameter for voice dialing, respectively. The user guide for each applicable telephone model describes the voice-initiated dialing user interface.

Gigabit Ethernet Adapter

As of Release 1.1, 9600 Series IP Telephones can accommodate a Gigabit Ethernet (GigE) Adapter. Release 1.5 introduced the 9630G and 9640G IP Telephones, which contain a built-in gigabit Ethernet adapter. Release 2.0 introduced the 9670G IP Telephone, which also contains a built-in gigabit Ethernet adapter. When connected to an adapter interface, the Gigabit Ethernet Adapter sets the Ethernet line interface operational mode that is built into the telephone to 1000Mbps full-duplex and deactivates the built-in secondary Ethernet interface. When a Gigabit Ethernet Adapter is present, any considerations or processing that apply to the "Ethernet line interface" apply only to the Ethernet line interface on that adapter. Likewise, any considerations or processing that apply to the "secondary Ethernet interface" apply only to the secondary Ethernet interface on the Gigabit Ethernet Adapter.

With an internal or connected Gigabit Ethernet Adapter, system parameters PHY1STAT (the Ethernet line interface) and PHY2STAT (the secondary Ethernet interface) activate the respective Ethernet interface in the 1000Mbps operational mode when supported by the hardware. When not supported by the hardware, the respective Ethernet interface is set to auto-negotiate the speed and duplex.

Dialing Methods

The 9600 Series IP Telephones have a variety of telephony-related applications that might obtain a telephone number during operation. For example, the Call Log saves the number of an incoming caller, but does not consider that the user has to then prepend the saved number with one or more digits to dial an outside line, and possibly one or more digits to dial long distance. Two dialing methods are used, depending on which version of Avaya Communication Manager (CM) is running.

Log Digit (Smart Enbloc) Dialing

Avaya Communication Manager (CM) Releases 4.0 and up give the call server the potential to provide a superior level of enhanced "log digit analysis." This feature (also called smart enbloc dialing) allows the call server to supplement the number the telephone dials based on the call server's knowledge of the entire dialing plan. With the server supporting log digit dialing analysis, the telephone does not attempt to enhance a number as described for enhanced local dialing, and the call server assumes responsibility for analysis and action. Smart enbloc provides a more accurate dialing method because the telephone signals to the call server that log dialing digit analysis is requested for all calls originated by the Redial buffer(s), the local Call Logs, and all web-based dialing.

Enhanced Local Dialing

For servers running a CM release earlier than 4.0, the 9600 Series IP Telephones evaluate a stored telephone number (other than those in the Contacts list) based on parameters administered in the settings file. The telephone can then automatically prepend the correct digits, saving the user time and effort. This is Enhanced Local Dialing. The key to the success of this feature is accurate administration of several important values, described in Table 11 and summarized below.

The system values relevant to the Enhanced Dialing Feature are:

- **ENHDIALSTAT** - Enhanced dialing status. If set to "1" (the default) the enhanced local dialing feature is turned on. If set to "0" enhanced local dialing is off. However, when in effect, Log Digit (Smart Enbloc) Dialing takes precedence, regardless of the ENHDIALSTAT setting.
- **PHNCC** - the international country code of the call server's location. This value is used in conjunction with the PHNIC value to help identify when a call to be dialed might be an international number. For example, set PHNCC to "1" when the call server is in the United States, to "44" for the United Kingdom, and so on.
- **PHNDPLENGTH** - the length of internal extension numbers. Used to help the telephone identify whether the number to be called is an outside number (which requires combining with PHNOL to get an outside line) or an internal line. As long as PHNDPLENGTH is less than the length of a national number (PHNLDLENGTH), the telephone can determine the difference between the two types of numbers. However, the telephone cannot determine the type of number when the extension is at least as long as the national telephone number
- **PHNIC** - the maximum number of digits, if any, dialed to access public network international trunks. This value is used in conjunction with the PHNCC value to help identify when a call to be dialed might be an international number. The country code is inserted if the number to be dialed includes a plus sign (+) followed by a country code

other than the one identified in PHNCC. However, the plus sign is almost never presented in calling or called party number data and usually only in Web-based click-to-dial links.

- **PHNLD** - the long distance access code; the digit dialed to access public network long distance trunks. If the number to be dialed is longer than the extension number length and equal in length to PHNLD, the telephone presumes it is a national number, and should be preceded by the long distance access code. For example, in the United States a 10 digit number includes the area code and must be preceded by a "1."
- **PHNLDLENGTH** - the maximum length, in digits, of the national telephone number for the country in which the call server is located. If the number to be dialed is longer than the extension number and is not equal to PHNLD, the number is presumed to be a subset of the national number and the long distance access code is not used.
- **PHNOL** - the character(s) dialed to access public network local trunks on the call server. If the number to be dialed is not an extension number, the telephone presumes it is an outside number which needs to be preceded by the code to access an outside line, commonly a "9".

Note:

As with any parameters in Table 11, the default values are used unless you explicitly administer different values. Thus, if you do not administer a given parameter, or if you comment a given parameter out in the 46xxsettings file, the default value for that parameter is used.

Important:

In all cases, the values you administer are the values applicable to the location of the call server. This means the site of the one Enterprise media server that handles multi-national locations. For example, if a telephone is located in London, England but its call server is in the United States, the **PHNCC** value needs to be set to “1" for the United States. If the call server is in London, PHNCC would be set to "44" even if the telephones it serves are in the United States.

Note:

In all cases, the digits the telephones insert and dial are subject to standard Avaya server features and administration. This includes Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), and so on.

As indicated in Table 11, you can administer the system parameter **ENHDIALSTAT** to turn off the Enhanced Local Dialing feature.

Example: A corporate voice network has a 4-digit dialing plan. The corporate WML Web site lists a 4-digit telephone number as a link on the Human Resources page. A 9620 user selects that link. The 9620 deduces the telephone number is part of the corporate network because the length of the telephone number is the same as the corporate dialing plan. The telephone dials the number without further processing.

Example: A user notes a Web site contains an international telephone number that needs to be

called and initiates the call. The telephone determines the number to be called is from another country code. The telephone then prepends the rest of the telephone number with PHNOL to get an outside line and PHNIC to get an international trunk. The telephone then dials normally, with the call server routing the call appropriately.

Enhanced Local Dialing Requirements

The enhanced local dialing feature is invoked when all the following conditions are met:

- A user invokes the Redial application, the Missed or Answered Call Log, or any Browser-based click-to-dial link to identify a telephone number to dial, and
- The Phone application determines a call appearance is available for an outgoing call, and
- The current value of ENHDIALSTAT is "1" (On), and
- The call server has not indicated it supports smart enbloc dialing (call type digit analysis available with Communication Manager Release 4.0 and later).

The Phone application takes the incoming character string, applies an algorithm, and determines the string of digits to be sent to automated call processing (ACP) for dialing. At this point the Phone application goes off-hook and sends the digits to ACP.

Note:

The Enhanced Local Dialing algorithm requires that telephone numbers be presented in a standard format. The standard format depends on how you administer the parameters indicated in Table 11. also described in Enhanced Local Dialing. The algorithm also assumes that international telephone numbers are identified as such in, for example, WML Web sites. This is indicated by preceding that type of number with a plus (+) sign, and a space or some non-digit character following the country code.

Administering Features on Softkeys

As of software Release 2.0, you can administer call server features on softkeys in the Phone application. The number of features you can place on a set of softkeys depends on the call state the telephone is presenting to the user.

The chart below lists the call states for which you can administer softkeys, the relevant system parameter associated with a call state, the maximum number of features you can specify in that system parameter, and the softkey numbers that can take administered features.

Call State	System Parameter	Maximum # of Features Allowed	Available Softkeys
Idle	IDLEFEATURES	6	All softkeys
Dialing	DIALFEATURES	5	1, 3, & 4

Active with ringback	RINGBKFEATURES	3	3
Active with talk path	TALKFEATURES	3	4

Note:

The system parameters are described in more detail in Table 11.

This capability works as follows:

- You administer feature buttons for the telephone on the call server as you normally would, and the call server sends these button assignments to the telephone as it always has.
- In the 46xxsettings file, you administer any or all of the system parameters indicated in the chart above. Each parameter consists of a list of one or more feature numbers, up to the maximum indicated in that chart, with each feature number corresponding to a specific administrable feature. Table 15 lists the administrable features and their associated numbers.
- The telephone compares the list of features you administered on the call server with the list of features in the system parameters you administered. Assuming a given feature occurs both in call server administration and in a given system parameter, that feature is displayed on a Phone application softkey when the highlighted call appearance is in the associated call state. The telephone displays the feature buttons starting with Softkey 1 and continuing to the right in the order specified in the system parameter, subject to the considerations listed in this section.

  Example:

  Assume call server administration includes the Send All Calls and Directory features. If the system parameter IDLEFEATURES is not administered, the corresponding softkeys are labeled from left to right as follows when a highlighted call appearance is Idle:

Redial	Send All	(blank)	(blank)

  However, when the system parameter IDLEFEATURES is administered to be "26,1000,35" the corresponding softkeys are labeled from left to right as follows when a highlighted call appearance is Idle:

Directory	Redial	Send All	(blank)

Softkeys available to be labeled with feature buttons as indicated under Available Softkeys in the page 117 chart are those that are not dedicated to a higher priority function. For example, in the "Active with a talk path" call state, the softkeys for Hold, Conference, and Transfer are dedicated to those functions and cannot be displaced by an administrable feature button, while the softkey normally labeled Drop (softkey #4) can be used for an administrable feature button.

In addition to the administrable feature numbers listed in Table 15, two additional "features" can be specified on a softkey of your choice or can be completely replaced. In the case of the system parameters IDLEFEATURES or DIALFEATURES, if the list of feature numbers includes the value 1000, the corresponding softkey is reserved for the Redial feature local to the telephone. This means the corresponding softkey is labeled Redial if the telephone has at least one phone number stored for the Redial feature -- otherwise the softkey is unlabeled. In the case of the system parameter IDLEFEATURES, if the list of feature numbers includes the value

1100, the corresponding softkey is reserved for a "Backlight Off" icon. When pressed, this softkey turns the telephone’s backlight off, saving energy. The backlight comes back on automatically when an phone activity is detected, such as an incoming call or a button press by the user.

Another consideration for IDLEFEATURES or DIALFEATURES is that if the system parameter PHNEMERGNUM is administered, the third softkey in the Idle or Dialing call state will always be labeled "Emerg." regardless of the contents of those system parameters.

Features administered only for any SBM24 Button Module are ignored. The feature must be administered for the telephone itself and not the button module.

Primary call appearances, bridged call appearances, and Team Buttons cannot be administered on softkeys.

The feature button softkey labels displayed to the user are those downloaded from the call server. If the user has personalized the labels, the personalized labels are presented instead.

If one of the designated parameters contains a Feature number more than once, and that number corresponds to at least one occurrence of a feature button downloaded from the call server, the designation of softkeys to features is assigned in the order the features are listed. For example, if two Abbreviated Dial (AD) buttons (Feature Number 65) are listed in the DIALFEATURES parameter, the first AD button in that list is associated with the first AD button downloaded from the call server. The second AD button in the DIALFEATURES parameter is associated with the second AD button downloaded from the call server (if any), and so on.

Note:

The system parameters allow you to specify more features than can be displayed on any one telephone. For example, IDLEFEATURES allows you to specify up to six features, although any one telephone can display at most four of them. The maximum size of each parameter allows you to specify one comprehensive list for that parameter’s related call state, but allows your user community to see different feature buttons depending on how you administer their telephones.

Since the telephone only displays feature button labels for features administered on the call server, you can set the softkey feature system parameters to values that will correspond to features for some users, but not others. For example, if TALKFEATURES is administered to "325,50", the users having Conference Display administered would see that label on softkey #3 for the Active with talk path call state, but users with Attendant Release would instead see that label on softkey #3. Since softkey labels display in the order in which they are administered in the system parameter, a user with both Conference Display and Attendant Release would only see a Conference Display softkey.

The Feature Numbers are as follows:

Table 15: CM Feature Numbers for Assigning Softkeys

Feature Name	Default Label	Feature Number
abr-prog	AbbrvDial Program	67
abr-spchar	AbrvDial (char)	68
abrv-dial	AD	65
abrv-ring	AR	226
ac-alarm	AC Alarm	128
aca-halt	Auto-Ckt Assure	77
account	Acct	134
act-tr-grp	Cont Act	46
admin	Admin	150
after-call	After Call Work	91
alrt-agchg	Alert Agent	225
alt-frl	Alt FRL	162
ani-requst	ANI Request	146
assist	Assist	90
asvn-halt	asvn-halt	214
atd-qcalls	AQC	89
atd-qtime	AQT	88
audix-rec	Audix Record	301
aut-msg-wt	Message (name or ext)	70
auto-cbk	Auto Callback	33
auto-icom	Auto (name or ext)	69
auto-in	Auto In	92
auto-wkup	Auto Wakeup	27
autodial	Autodial	227
aux-work	Auxiliary Work	52
btn-ring	Button Ring	258
btn-view	Button View	151

1 of 7

Table 15: CM Feature Numbers for Assigning Softkeys (continued)

Feature Name	Default Label	Feature Number
busy-ind	Busy	39
call-disp	Make Call	16
call-fwd	Call Forwarding	74
call-park	Call Park	45
call-pkup	Call Pickup	34
callr-info	Caller Info	141
call-timer	Ctime	243
cancel	Cancel	51
cas-backup	CAS Backup	76
cdr1-alrm	CDR 1 Failure	106
cdr2-alrm	CDR 2 Failure	117
cfwd-bsyda	Call Forwarding bsyda (ext)	84
cfwd-enh	Call Forwarding Enhanced	304
check-in	Check In	29
check-out	Check Out	28
class-rstr	COR	59
clk-overid	Clocked Override	112
conf-dsp	Conference Display	325
con-stat	Console Status	185
consult	Consult	42
cov-cback	Coverage Callback	17
cov-msg-rt	Cover Msg Retrieve	12
cpn-blk	CPN Block	164
cpn-unblk	CPN Unblock	165
crss-alert	Crisis Alert	247
cw-ringoff	CW Aud Off	62
date-time	Date Time	23
deact-tr-g	Cont Deact	47
delete-msg	Delete Message	14

2 of 7

Table 15: CM Feature Numbers for Assigning Softkeys (continued)

Feature Name	Default Label	Feature Number
dial-icom	Dial Icom	32
did-remove	DID Remove	276
did-view	DID View	256
directory	Directory	26
dir-pkup	Directory Pkup	230
disp-chrg	Display Charge	232
display	Display	180
disp-norm	Local/Normal	124
dn-dst	Do Not Disturb	99
dont-split	Don’t Split	176
dtgs-stat	DTGS Status	181
ec500	Extension to Cellular	335
em-acc-att	Emerg Access to Attd	64
exclusion	Exclusion	41
ext-dn-dst	Do Not Disturb Ext.	95
extnd-call	Extend Call	345
fe-mute	Far End Mute for Conf	328
flash	Flash	110
forced-rel	Forced Release	57
goto-cover	Go To Cover	36
group-disp	Group Display	212
group-sel	Group Select	213
grp-dn-dst	Do Not Disturb Grp	96
grp-page	GrpPg	135
headset	Headset	241
hundrd-sel	Group Select #	58
hunt-ne	Hunt Group	101
in-call-id	Coverage (Info)	30
in-ringoff	In Aud Off	60

3 of 7

Table 15: CM Feature Numbers for Assigning Softkeys (continued)

Feature Name	Default Label	Feature Number
inspect	Inspect Mode	21
int-aut-an	IntAutoAns	108
intrusion	Intrusion	179
last-mess	Last Message	182
last-numb	Last Number Dialed	66
last-op	Last Operation	183
lic-error	License Error	312
limit-call	LimitInCalls	302
link-alarm	Link Failure (#)	103
local-tgs	Local-tgs (#)	48
lsvn-halt	Login SVN	144
lwc-cancel	Cancel LWC	19
lwc-lock	Lock LWC	18
lwc-store	LWC	10
maid-stat	Maid Status	209
major-alrm	Major Hdwe Failure	104
man-msg-wt	Msg Wait (name or ext.)	38
man-overid	Immediate Override	113
manual-in	Manual In	93
mct-act	MCT Activation	160
mct-contr	MCT Control	161
mf-da-intl	Directory Assistance	246
mf-op-intl	CO Attendant	229
mj/mn-alrm	Maj/Min Hdwe Failure	82
mm-basic	MM Basic	169
mm-call	MM Call	167
mm-cfwd	MM CallFwd	244
mm-datacnf	MM Datacnf	168
mmi-cp-alm	MMI Circuit Pack Alarm	132

4 of 7

Table 15: CM Feature Numbers for Assigning Softkeys (continued)

Feature Name	Default Label	Feature Number
mm-multnbr	MM MultNbr	170
mm-pcaudio	MM PCAudio	166
msg-retr	Message Retrieve	11
mwn-act	Message Waiting Act.	97
mwn-deact	Message Waiting Deact.	98
next	Next	13
night-serv	Night Serv	53
noans-alrt	RONA	192
no-hld-cnf	No Hold Conference	337
normal	Nornal Mode	15
occ-rooms	Occ-Rooms	210
off-bd-alm	Offboard Alarm	126
override	Attndt Override	178
per-COline	CO Line (#)	31
pms-alarm	PMS Failure	105
pos-avail	Position Available	54
pos-busy	Position Busy	119
post-msgs	Post Messages	336
pr-awu-alm	Auto Wakeup Alm	116
pr-pms-alm	PMS Ptr Alarm	115
pr-sys-alm	Sys Ptr Alarm	120
print-msgs	Print Msgs	71
priority	Priority	81
q-calls	NQC	87
q-time	OQT	86
release	Attendant Release	50
release	Station Release	94
remote-tgs	Remote TG (#)	78
re-ringoff	Ringer Reminder	61

5 of 7

Table 15: CM Feature Numbers for Assigning Softkeys (continued)

Feature Name	Default Label	Feature Number
ringer-off	Ringer Cutoff	80
rs-alert	System Reset Alert	109
rsvn-halt	rsvn-halt	145
scroll	Scroll	125
send-calls	Send All Calls	35
send-term	Send All Calls-TEG	72
serial-cal	Serial Call	177
serv-obsrv	Service Observing	85
signal	Signal (name or ext.)	37
split	Split	56
split-swap	Split-swap	191
ssvn-halt	ssvn-halt	231
sta-lock	Station Lock	300
start	Start Call	55
stored-num	Stored Number	22
stroke-cnt	Stroke Count (#)	129
term-x-gr	Term Grp (name or ext.)	40
togle-swap	Conf/Trans Toggle-Swap	327
trk-ac-alm	FTC Alarm	121
trk-id	Trunk ID	63
trunk-name	Trunk Name	111
trunk-ns	Trunk Group	102
usr-addbsy	Add Busy Indicator	239
usr-rembsy	Remove busy Indicator	240
uui-info	UUI-Info	228
vc-cp-alm	VC Circuit Pack Alarm	133
verify	Verify	75
vip-chkin	VIP Check-in	277
vip-retry	VIP Retry	148

6 of 7

Table 15: CM Feature Numbers for Assigning Softkeys (continued)

Feature Name	Default Label	Feature Number
vip-wakeup	VIP Wakeup	147
vis	vis	184
voa-repeat	VOA Repeat	208
voice-mail	Message	326
vu-display	VuStats #	211
whisp-act	Whisper Page Activation	136
whisp-anbk	Answerback	137
whsp-off	Whisper Page Off	138
work-code	Work Code	140

7 of 7

Administering a Custom Screen Saver

Avaya provides a standard screen saver, however, you can administer a customized screen saver for 9600 Series IP Telephones with bit-mapped displays. The screen saver displays when the idle timer reaches the value set in the system parameter SCREENSAVERON. The screen saver is removed whenever the idle timer is reset. If the value of SCREENSAVERON is "0", neither the standard Avaya screen saver, nor any customized screen saver you specify in the SCREENSAVER system parameter will be displayed.

Screen savers display for approximately 5 seconds at a time at random locations on the screen, such that the entire image is always displayed. When the screen saver is removed, the previously displayed screen is restored unless another screen is appropriate due to a specified software operation such as making a call from the Phone screen.

You can administer color images for gray-scale sets, or black and white images for color sets. The telephone will present the images as applicable for their individual displays.

To determine what image to display, the telephone follows this procedure:

1. During boot-up the telephone checks for the file named in the system parameter SCREENSAVER. If found, that file is checked for valid jpeg format, and to verify that the screen saver image height and width do not exceed the applicable full screen pixel count of 160x160 for a 9610, 160x320 for a 9620, or 320x240 for a 9630, 9640 or 9650, or 480x640 for a 9670G IP Telephone. Note that the screen saver should be a smaller size than these pixel values specified so it can move randomly while displaying the entire image.

2. If no valid file was downloaded, either because no file exists, or because the downloaded file exceeded one or more of the pixel count limits, or because the image is not a valid JPEG image, the Avaya-specific screen saver is used.

The best way to use the SCREENSAVER parameter is to administer different file names in the 46xxsettings file, listed under different MODEL4 values (9620, 9630, etc.). In other words, using the MODEL4 IF statements, you can administrator a given telephone to point to a unique SCREENSAVER value that is appropriate for that telephone.

Backup/Restore

Note:

This section does not apply to the 9610 IP Telephone. For 9610 backup/restore information, see Special Administration for the 9610 IP Telephone.

The 9600 Series IP Telephones support the HTTP client to back up and restore the user-specific data indicated in Table 17. As of Software Release 1.5, HTTP over TLS (HTTPS) is also supported for backup/restore. For backup, the telephone creates a file with all the user-specific data if a backup file location is specified in system parameter BRURI. The file is sent to the server by an HTTP PUT message, with appropriate success or failure confirmation.

For restore, the initiating process must supply only the backup file name. The file is requested from the server by an HTTP GET message. If successful, the file is returned to the initiating process, otherwise a failure message is returned.

Backup and restore operations construct the URI used in the HTTP message from the value of the BRURI parameter and from the file name as follows:

- If BRURI ends with **/** (a forward slash), the file name is appended.
- Otherwise, a forward slash is appended to the BRURI value, then the file name is appended to that.

Note:

BRURI can include a directory path and/or a port number as specified in IETF RFCs 2396 and 3986.

If TLS is used, the telephone's call server registration password can be included in an Authorization request-header in each transmitted GET and PUT method. This is intended for use by the Avaya IP Telephone File Server Application (which can be downloaded from the Avaya support Web site) so that the telephone requesting the file transaction can be authenticated.

If no digital certificates have been downloaded based on the system parameter TRUSTCERTS, the telephone establishes a TLS connection only to a backup/restore file server that has a Avaya-signed certificate (which is included by default with the Avaya IP Telephone File Server Application), and the credentials are always included. However, if at least one digital certificate

has been downloaded based on TRUSTCERTS, the credentials are included only if BRAUTH is set to "1". This is a security feature to allow control over whether the credentials are sent to servers with third-party certificates. If a non-Avaya certificate is used by the server on which the Avaya IP Telephone File Server Application is installed, set BRAUTH to "1" to enable authentication of the telephones. The default value of BRAUTH is "0".

When the call server IP address and the telephone's registration password are included as the credentials in an Authorization request-header, the call server IP address is included first in dotted-decimal format, followed by a colon (hex 3A), followed by the telephone's registration password.

HTTP/HTTPS authentication is supported for both backup and restore operations. The authentication credentials and realm are stored in re-programmable, non-volatile memory, which is not overwritten when new telephone software is downloaded. Both the authentication credentials and realm have a default value of null, set at manufacture or at any other time user-specific data is removed from the telephone. When TLS is used, the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is used for authentication. If the digital certificate of the server is signed by the Avaya Product Root Certificate Authority certificate, the telephone's call server registration password is included as the credentials in an Authorization request-header for each transmitted PUT (backup) and GET (for restore) method.

New value(s) replace the currently stored authentication and realm values:

- when HTTP authentication for backup or restore succeeds and
- if the userid, password, or realm used differs from those currently stored in the telephone.

If HTTP authentication fails, the user is prompted to enter new credentials.

Note:

Users can request a backup or restore using the Advanced Options Backup/ Restore screen, as detailed in the user guide for their specific telephone model. For specific error messages relating to Backup/Restore, see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

Backup

When the system parameter BRURI is non-null, user changes are automatically backed up to the file **ext_96xxdata.txt** (where **ext** is the value of NVPHONEXT) on the HTTP server to a user-specified directory. Backup formats are as follows:

Table 16: Backup File Formats

Item/Data Value	Format
Generic	*name=value*
Contacts	ABKNAME*mmm*=ENTRY_NAME ABKNUMBER*mmm*=ENTRY_NUMBER_1 ABKTYPE*mmm*=ENTRY_TYPE (where *mmm* is the one-, two-, or three-digit entry ID, with leading zeros for single and double-digit entry IDs)
Call Log entries	CLNAME*mmm*=ENTRY_NAME CLNUMBER*mmm*=ENTRY_NUMBER CLTYPE*mmm*=ENTRY_TYPE CLDATE*mmm*=ENTRY_DATE CLTIME*mmm*=ENTRY_TIME CLDURATION*mmm*=ENTRY_DURATION CLBRIDGEDFLAG*mmm*=ENTRY_BRIDGEDFLAG CLMISSEDCNTR*mmm*=ENTRY_COUNTER CLBCALBL*mmm*=ENTRY_BCALBL To be valid, a Call Log entry must have at least a non-null Date and Type, and either Name or Number (or both) must be non-null.
User-generated Call Appearance labels with button identifiers of *mm* (the one- or two-digit button number of the entry with a lead zero for single-digit numbers)	PHNLABEL*mm*=CAUSERLABEL
User-generated telephone Feature Button labels with button identifiers of *mm* (the one- or two-digit button number of the entry with a lead zero for single-digit numbers)	PHNLABEL*mm*=FBUSERLABEL
User-generated SBM24 Call Appearance or Feature Button labels with button identifiers of *mm* (the one- or two-digit button number of the entry with a lead zero for single-digit numbers)	SBMLABEL*mm*=CAUSERLABEL or FBUSERLABEL, as applicable

A backup saves the options and non-password parameters shown in Table 17, as well as the information shown in Table 16.

Table 17: Options and Non-Password Parameters Saved During Backup

Parameter Name	Setting
HOMEFAV*nn*	Contact Favorites data; 9670G only. An entry is backed up for each Home screen favorite, where *nn* is the index number for that favorite. The backup file format for a Favorite is: HOMEFAVnn=Fav_Number<US>Fav_Caption<US>Contact_Name where Fav_Number is the phone number associated with the Favorite, Fav_Caption is the Favorite's caption text, Contact_Name is the Name for the associated Contact entry, and <US> is the Unit Separator (0x001F Unicode value). Upon Restore, a link must be established between a Favorite and a Contact entry by matching the Contact_Name against a Contact's Name and Fav_Number against one of that Contact's numbers. If no match is found, then the Favorite cannot be restored and is discarded.
LANGUSER	Display Language
LOGACTIVE	Call Log Active
LOGBRIDGED	Log Bridged Calls
LOGTDFORMAT	Call Log Data Time/Date Format
OPTAGCHAND	Handset Automatic Gain Control
OPTAGCHEAD	Headset Automatic Gain Control
OPTAGCSPKR	Speaker Automatic Gain Control
OPTAUDIOPATH	Audio Path
OPTCLICKS	Button Clicks
OPTERRORTONE	Error Tones
OPTGUESTLOGIN	Guest Login Permitted/Not Permitted
OPTHOMEIDLE	Home Screen on idle; 9670G only
OPTTEXTSIZE	Text Size
PERSONALRING	Personalized Ring Note for the 9670G only: this value is backed up as equal to the PERSONALWAV value when PERSONALWAV is set to one of the 8 standard ring patterns. When PERSONALWAV is greater than 8 (meaning it is set to one of the newer ring patterns) and PERSONALRING was set using a backup file value, that backup value is re-saved. If neither of these conditions apply, no PERSONALRING value is backed up.

Table 17: Options and Non-Password Parameters Saved During Backup (continued)

Parameter Name	Setting
PERSONALWAV	Personalized Ring value - 9670G only
PHNABKNAME	Contacts Pairing
PHNEDITDIAL	Edit Dialling
PHNQUICKPANEL	Quick Touch Panel; 9670G only
PHNREDIAL	Redial
PHNSCRONANS	Go to Phone Screen on Answer
PHNSCRONCALL	Go to Phone Screen on Calling
PHNSCRONALERT	Go to Phone Screen on Ringing
PHNTIMERS	Call Timer
PHNVBDIALSTAT	Voice Initiated Dialing
PHNVBDIALLANG	Voice Initiated Dialing Language
PHNVISUALALERT	Visual Alerting
PRINGMENU	Personalized Ring Menu
VIDHELP	Voice Initiated Dialing Help Counter
WEATHERLOCID	Weather Location ID; 9670G only
WEATHERUNITS	English/Metric; 9670G only
WORLDCLOCKLIST	List of World Clock location entries; 9670G only

Restore

When automatic or user-requested retrieval of backup data is initiated, system values and internal values are set to values contained in the backup file. This occurs only if the OPSTAT parameter setting allows the user to change those values. Therefore, any restrictions set using OPSTAT are recognized and honored.

The backup file value is not retrieved, and the current setting remains valid:

- when a value in the backup file has changed and
- that value corresponds to an application that OPSTAT indicates should not be changed.

This prevents a user from bypassing the administration of OPSTAT and changing options settings in the backup file.

Note:

If you administered the APPSTAT parameter to suppress changes to one or more applications, the telephone backs up and restores data as usual, but ignores data for “suppressed” applications. This prevents a user from bypassing your APPSTAT restrictions by editing the backup file. For information about APPSTAT, see The Application Status Flag (APPSTAT) on page 144.

During backup file restoration, user activity is prohibited until a `Retrieval successful` or `Retrieval Failed` message displays. When a restore attempt fails, if a retrieved file has no valid data, or if a retrieved file cannot be successfully stored, a `Retrieval Failed` message displays at the telephone until the user takes another action.

Data retrieval considerations are as follows:

- When you create a backup file rather than edit an existing one, be sure to create the file with UTF-16 LE (little endian) characters, with Byte Order Mark (BOM) for LE of 0xFFFE.
- Backup saves data values using the generic format *name*=*value*. For specific formats, see Backup.
- All identifiers, for example, *names*, are interpreted in a case-insensitive manner, but the case of parameter values, Contact names, and numbers is preserved.
- Spaces preceding, within, or following a *name* are treated as part of the *name*.
- <CR> and <LF> (UTF-16 characters 0x000D and 0x000A, respectively) are interpreted as line termination characters.
- Blank lines are ignored.
- When an identifier is not recognized or is invalid, the entire line is ignored. Likewise, if an identifier is valid but the data itself is invalid or incomplete, the line is ignored.
- When an identifier is valid with valid and complete data, but the data is not applicable to the current state of the telephone, the data is retained for possible use later, and is considered data to be backed up at the appropriate time. For example, if button labels for an SBM24 button module unit are present, but no such module is attached to the telephone, the button labels are retained.
- When more than one line contains a value for an option, parameter, or Contacts entry, the last value read is retrieved, to allow new values to overwrite previous values as lines are read from the backup file. In all other cases, the line order in the backup file has no bearing on retrieval.
- The existence of invalid data does not constitute a failed retrieval. The success of the retrieval process requires the telephone to obtain the backup file and successfully restore valid data.

9610 Backup/Restore

The 9610 uses its backup/restore functionality differently than other 9600 Series IP Telephones. There is no user-created data nor are there options that need to be stored in a 9610 backup file. The 9610 uses its backup file as the source for administration of the button labels and associated telephone numbers in the Contacts application, the Main Menu list, and associated data, etc.

The administrator is expected to build the backup file in accordance with the requirements in this section, so that when the 9610 boots up and registers, it will obtain the appropriate data for user presentation.

Differences with the backup/restore procedures used on the other 9600 Series IP Telephones include:

- The 9610 never “backs up” data, it only retrieves data. Since the user has no mechanism to change any data, there is no need to back up changes. For consistent terminology with other 9600 Series IP Telephones, we use the term “backup file” here for the 9610 file.
- Because the user can never change data, the OPSTAT value is ignored for the purposes of populating the display from the 9610 backup file.
- When the 9610 attempts to retrieve the backup file, the telephone first attempts to retrieve a file labeled **ext_9610data.txt**. If the 9610 does not retrieve this file successfully, unlike the other 96xx sets, the 9610 attempts to retrieve a file labeled **9610data.txt**. This file does not have an extension designation. This retrieval process has the advantage of allowing all 9610s that are not associated with a specific extension’s backup file to share a common backup file. You can have, for example, three unique 9610 backup files - one for a 9610 in the Marketing conference room, one for a 9610 in the Accounting conference room, and one for five 9610 IP Telephones in public areas of the company.

9610 Retrieval Procedures

When the telephone initiates an automatic retrieval, the telephone first attempts to retrieve a file with filename ***ext*_9610data.txt**, where ***ext*** is the system value of NVPHONEXT. While in progress, the Top Line displays **Retrieval 1**. If the file is retrieved successfully, the Top Line displays **File obtained** while the telephone validates the data, and stores valid data in memory. All previous corresponding data is replaced, unless the restore fails, as described below. When data storage is completed successfully, the Top Line displays **Restore OK** for 30 seconds, or until the user selects another Application Line or application, whichever comes first.

If this first retrieval attempt fails for any reason, or if the successfully retrieved file had no valid data, the 9610 then attempts to retrieve a file with the filename **9610data.txt**. While this retrieval is in progress, the Top Line displays **Retrieval 2**. If the file is retrieved successfully the remaining steps are identical to those for the ***ext*_9610data.txt** file.

If:

- this second retrieval attempt fails for any reason, or
- the file is successfully retrieved but has no valid data, or
- either successfully-retrieved file was not successfully stored, then

the Top Line displays **Restore failed** for 30 seconds, or until the user selects another Application Line or application, whichever comes first. Once the data storage starts and until the **Restore OK** or **Restore failed** message displays, the user cannot perform any action to display another screen, for example, the Avaya Menu button is temporarily locked out and any press of it is ignored. Once the appropriate result message is displayed, the corresponding 9610 user interface is presented.

General 9610 Restore Processing

Characters are assumed to be coded in UTF-16 LE (little-endian, with Byte Order Mark (BOM) for LE (0xFFFE)), with each item on a separate line terminated by" <CR><LF>" (000D 000A in UTF-16) characters.

Important:
If the file is not in this format, the telephone displays the message "`Restore failed.`".

The generic format for data values is: *name*=*value*.

The format for retrieving a Main Menu entry is:

MMLBLxx =*entry label*
MMTYPExx =*entry type*
MMDATAxx =*entry data*

For more information, see Main Menu (MM) Administration on page 170.

The format for retrieving a Contacts entry is:

CONLABELxxx = *entry label*
CONDATAxxx = *entry data*

For more information, see Contacts Application Administration on page 171.

The other parameters that have meaning in a 9610 backup file are:

IDLEAPP- as described in The 9610 Idle Application, WMLIDLETIME, SCREENSAVERON, IDLEAPP, and WMLSMALL on page 171.

LISTAPP - when LISTAPP is null (the default), the assumption is the administrator has not created an external equivalent to the local Contacts application. The local Contacts application is used unless it too is empty. When the local Contacts application is empty, selecting **List** is the same as pressing the **Start** button. When LISTAPP is non-null, the assumption is the administrator has populated it with a URI for a WML-based application to be displayed when **List** is selected.

When retrieving data, the following applies:

- If the Byte Order Mark (BOM) is not 0xFFFE, the entire file is rejected and the retrieval fails.
- All identifiers, for example, names, are interpreted in a case-insensitive manner.
- The case of parameter values and Contacts names and numbers are preserved.
- Spaces preceding, within, or following a *name* or *value* are treated as part of that entity.
- <CR> and <LF> are interpreted as line termination characters.
- Blank lines are ignored.
- If an identifier is not recognized or is invalid, the entire line is ignored.

- If an identifier is valid but the data itself is invalid or incomplete, the line is ignored. The determination of what constitutes a valid value for each data element is specified in General 9610 Restore Processing and Backup File Format.
- If more than one line contains a value for a parameter or Contacts entry, the last value read is used (hence, new values overwrite previous values as lines are read from the file). In all other cases, the order of the lines in the file does not matter.

The success of the retrieval process requires the telephone to obtain the backup file, and to successfully store valid data. The existence of invalid data does not constitute a failed retrieval.

Note:

Chapter 9: Administering Specific 9600 Series IP Telephones describes 9610-specific administration.

Chapter 8: Administering Applications and Options

Customizing 9600 Series IP Telephone Applications and Options

The 9600 Series IP Telephones have some unique and powerful capabilities that take advantage of their display and access to LAN facilities. If your LAN has a WML Web site, the telephone needs key information about the servers providing those facilities. You need to provide the information called for in relevant sections of Table 18 in a customized script file. For more information, see 9600 Series IP Telephone Scripts and Application Files on page 80.

CAUTION:

For the telephones to work properly, you must have a *46xxsettings.txt* file in the same directory as the application file. If you do not edit the 46xxsettings.txt file, those telephones use default settings only. The 46xxsettings file is available as a standalone download. If you already have such a file because you downloaded it for a previous 9600 Series or 4600 Series IP Telephone release, installing the standalone file overwrites the original file.

Note:

To facilitate administration, the 9600 Series and 4600 Series IP Telephones use the same ***46xxsettings.txt*** file.

In Table 18, parameters shown with a **Mandatory** status must be accurate and non-null for the application to work. You can change parameters with an **Optional** status to suit your environment. If you do not change parameters, the defaults are used.

Table 18: 9600 Series IP Telephone Customizable System Parameters

Parameter Name	Default Value	Status	Description and Value Range
General User Parameters:			
APPSTAT	1	Optional	Applications status flag. See The Application Status Flag (APPSTAT) on page 144 for a description. See Table 19 for the range of values.
OPSTAT	111	Optional	Options status flag(s) (1 or 3 ASCII numeric digits) indicate which options are user-selectable. The default of 111 grants access to all options and related applications. Single digit valid values are: 1=user can access all options, including Logout, 2= user can access only view-oriented applications. Three-digit valid values are a concatenation of binary values, in the form *abc*, where each letter represents a 0 (disabled/off) or 1 (enabled/on), interpreted as: *a* = base settings for all user options and related applications, except as noted in *b* or *c*. *b* = setting for view-oriented applications (for example, the Network Information application), as applicable. *c* = setting for Logout application, if applicable. The binary "0" does not allow an end user to see or invoke options and related applications. The binary "1" allows full display and access to all options and related applications.
OPSTAT2	0		OPSTAT override flag. If set to 0, OPSTAT is not affected. If set to 1, OPSTAT is unaffected with the exception that any changes to customized labels in the backup file are uploaded and used as if OPSTAT permitted this action.

1 of 7

Table 18: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
Call Log Parameters:			
CLDELCALLBK	0	Optional	Delete calls from the Missed Call Log when the user returns the call from the Call Log? Values are 1=No, 0=Yes.
LOGBACKUP	1	Optional	Back up the user's Call Log? Values are: 1=Yes;the Call Log is backed up to the same backup file as all other user data (see Table 16 for information), subject to normal administration of that file. 0=No.
LOGMISSEDONCE	0	Optional	Maintain only one Call Log entry for multiple Missed calls from the same originating phone number. Values are: 1=Yes; each Missed Call Log entry is maintained, along with a Missed Call counter that tracks the number of times (up to 99) the originating number called. 0=No; each Missed Call creates a new Call Log entry.
LOGUNSEEN	0	Optional	Maintain a Call Log entry for calls that are redirected from the telephone, for example, Call forwarded calls? Values are: 1=Yes; 0=No. **Note:** CM 5.2 or later is required for this feature to work.

2 of 7

Table 18: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
Web Access Application Parameters:			
SUBSCRIBELIST	" " (Null)	Optional	Subscription list for potential pushed content. List of zero or more fully qualified URLs, separated by commas without intervening spaces, with up to 255 total characters.
TPSLIST	" " (Null)	Optional	List of Trusted Push Servers. List of zero or more fully qualified domain/path strings, separated by commas without intervening spaces, with up to 255 total characters. For more information, see the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-600888).
WMLHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Web Access application. Not applicable to the 9610, which uses WMLSMALL instead.
WMLPROXY	" " (Null)	Optional	Text string containing the IP Address, in dotted decimal or DNS format, of an HTTP proxy server. This parameter is optional if the Web pages a user accesses are all on the intranet of your organization.
WMLEXCEPT	" " (Null)	Optional	Text string containing a list of one or more HTTP proxy server exception domains, separated by commas, up to a total of 127 ASCII characters. This parameter is optional if the Web pages to be accessed by the user are all on the intranet of your organization. If WMLPROXY is null, the value of this parameter is ignored.

3 of 7

Table 18: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
WMLIDLETIME	10	Optional	Idle time before displaying Web page. The number of minutes of inactivity after which the Web browser will be displayed if WMLIDLEURI is not null. The default is 10 minutes. Valid values range from 1 to 999 minutes (16.65 hours).
WMLIDLEURI	" " (Null)	Optional	Idle time Web page URI. URI that specifies the Web page the browser displays after an idle interval. Value: Zero or one URI (0-255 ASCII characters, no spaces). Null is valid but if Null, no page displays. Avaya recommends that WMLIDLEURI be specified for phones in public areas through the use of a GROUP parameter. The idle timer is only reset if WMLIDLEURI is non-null such that an HTTP GET can be sent.
WMLPORT	80	Optional	Text string containing the TCP port number for the HTTP proxy server. The default is the TCP default for HTTP. This parameter is optional if the Web pages to be accessed by the user are all on the intranet of your organization. If WMLPROXY is null, the value of this parameter is ignored.
WMLSMALL	" " (Null)	Optional	Home page for the 9610 WML browser (only). Zero (0) to 255 ASCII characters = 1 or one URL. This parameter must be non-null for Main Menu WML links to be displayed. Other 9600 Series telephones use WMLHOME instead.

4 of 7

Table 18: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
Backup/Restore Parameters:			
BRURI	" " (Null)	Mandatory	URL used for backup and retrieval of user data. Specify HTTP server and directory path to backup file. Do not specify backup file name. Value: 0-255 ASCII characters. Null is a valid value and spaces are allowed. If this value is null or begins with a character sequence other than *http://* or *https://* the Backup/Restore option will not display to the telephone user.
Backlight Parameters:			
BAKLIGHTOFF	120	Optional	Number of idle minutes after which the backlight turns off (1-3 ASCII digits, from 0-999).
Guest Login Parameters:			
GUESTDURATION	2	Optional	Number of hours (1-12) a guest login is effective.
GUESTLOGINSTAT	0	Optional	Indicates whether a user can log in to a telephone as a guest. (Values are 0=the user is not allowed to use the Guest Login feature; 1=the user is allowed to use the Guest Login feature.
GUESTLOGINWARNING	5	Optional	Number of minutes in which the GUESTDURATION will expire. The valid range is 1 to 15 minutes.
Options Parameters:			
RINGTONESTYLE	0	Optional	Ring Tone Style Menu initially offered to the user (0=Classic; 1=Alternate).

5 of 7

Table 18: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
Phone Parameters:			
FBONCASCREEN	0	Optional	For the 9630/9630G/9640/9640G IP Telephones, display feature buttons on available lines on the Call Appearance (Phone) screen? Values are: 1=Yes; 0=No.
VPN Parameters:			
VPN parameters are listed in Appendix D: Administering a Virtual Private Network (VPN), and in Table 11: 9600 Series IP Telephone Customizable System Parameters.			
World Clock Application Parameters (9670G only):			
WMLPROXY	" " (Null)	Optional	Text string containing the IP Address, in dotted decimal or DNS format, of your corporate proxy server through which one accesses external Web sites. The World Clock application requires access to an external Web site to retrieve data.
WMLPORT	HTTP	Optional	Text string containing the TCP port number for the HTTP proxy server.
WORLDCLOCKAPP	"default"	Optional	Indicator to enable/disable the World Clock application. Valid values are: " " = Null; Disabled - do not show the World Clock application on the 9670G Home screen. Any text string other than null (" ") = Enabled; show the World Clock application on the 9670G Home screen.
Weather Application Parameters (9670G only):			
WMLPROXY	" " (Null)	Optional	Text string containing the IP Address, in dotted decimal or DNS format, of your corporate proxy server through which one accesses external Web sites. The Weather application requires access to an external Web site to retrieve data.
WMLPORT	HTTP	Optional	Text string containing the TCP port number for the HTTP proxy server.

Table 18: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
WEATHERAPP	"default"	Optional	Indicator to enable/disable the Weather application for 9670G IP Telephones only. Valid values are: Null = Disabled; do not show the Weather application on the Home screen. Any text string other than null = Enabled; show the Weather application on the Home screen.

7 of 7

Note:

The *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-600888) provides assistance in developing local Web sites.

The Application Status Flag (APPSTAT)

The 9600 Series IP Telephones offer the user numerous applications like Contacts, Call Log, Redial, and so on. Each of these applications allows the user to add, delete, or in some cases, edit entries. You, as the administrator, might not want the user to have that level of functionality. For example, a hotel lobby telephone probably should not allow a user to delete the concierge's contact number. Further, for privacy reasons, that same telephone should not allow a Call Log display. You can use the Application Status Flag, APPSTAT, to administer specific application functionality permission levels for one or more telephones.

APPSTAT consists of one number, specifying a certain level of allowed functionality. A Zero ("0") value is the most limiting setting. Values "2" and "3" allow increasing levels of functionality, and "1" allows the user complete application functionality.

Table 19: Application Status Flags and Their Meaning

APPSTAT Value	Meaning
0	Redial and Call Log are suppressed. Contact changes are not allowed.
1	***All administered applications are displayed, with full functionality. This is the default value.***
2	Call Log is suppressed. Contact changes are not allowed. Only one-number Redial is allowed.
3	Contact changes are not allowed. For the 9670G, this also means that users cannot assign or remove contact Favorites via the Home screen.

In Table 19, “suppressed” applications are not displayed to the user. Softkey labels, application tabs, and so on are not labeled or displayed. Options associated with suppressed applications can continue to display unless you override them by appropriate OPSTAT parameter administration. Displayed options have no effect while the application is suppressed.

In Table 19, “Contact changes are not allowed” means the Contact application displays and the user can make calls as normal. Any controls that allow the user to change any aspect of the Contact application do not display. This restriction includes the ability to add, delete, or edit any Contact name or number.

In Table 19, “Only one-number Redial is allowed” means the user Option that allows a choice between displaying last numbers dialed is suppressed. The Redial buffer stores only one number. The Redial application does not display since the user can redial only one number. This restriction allows privacy once a given user has left the telephone.

You can:

- set **APPSTAT** to **1**, for example, in a staging area,
- administer a given telephone with Contact entries of your choice, like the **Concierge telephone number** button in the earlier example,
- then move the telephone to where it will be used, where you have administered APPSTAT to be, for example, 0 (zero).

When the relocated telephone resets, it retains its Contact entries, like Concierge, but does not allow the user to create new entries.

When you set APPSTAT to any valid value other than 1, the telephone does not accept any Contact button label changes that might have been made directly on a backup file. Only the existing labels of the telephone are used. This restriction prevents circumvention of the APPSTAT restrictions. The WML applications are also suppressed by default.

Special Administration for the 9610

Administration of the 9610 IP Telephone is handled using the restore file rather than the settings file which is used by all other 9600 Series IP Telephones. For information, see 9610 Backup/ Restore on page 132.

Special Administration for the 9670G

The 9670G is a touch-based phone, and as such, uses a touch-based Home Screen in place of the Avaya Menu that other 9600 Series IP Telephones use. The Home Screen provides access to telephone options and settings, special Avaya applications like a World Clock and Weather,

Contact Favorites, and any WML applications you may administer. The Home screen can display up to four WML applications, but if you have configured more than four applications, **More** displays to provide access to all WML applications. See WML Application Display on the 9670G Home Screen for information about display characteristics and icons. If there are no WML applications, there may be a single WML Browser item shown, providing the system parameter WMLHOME is set with a value. Most Avaya Menu elements like those for WML applications do apply, and any 9670G exceptions are noted where applicable in the appropriate sections under Avaya "A" Menu Administration.

Avaya "A" Menu Administration

Release 1.2 provided a new user interface (UI) that put multiple WML applications in the first level of the “A” (Avaya) Menu. The A (Avaya) Menu is a list of sub-applications the user can select from to invoke the corresponding functionality. A new file called AvayaMenuAdmin.txt is available with Release 1.2 and greater downloads on which you can specify the menu label, URI, and list order of WML applications on the “A” Menu.

Software Release 2.0 added a Home screen that replaces the A Menu for the 9670G IP Telephone only. The addition of the 9670G model requires that the AvayaMenuAdmin.txt file be used to specify the WML applications you want displayed on the 9670G Home screen. These applications are displayed in order from left to right, going to a second page if necessary.

Note:

This section applies to all 9600 Series IP Telephones except the 9610. For information on 9610 IP Telephone menu administration, see Special Administration for the 9610 IP Telephone in Chapter 9.

Note:

The 9670G has a unique Home Screen that replaces the Avaya Menu for access to menu options and settings, log out, Bluetooth setup, and touch screen cleaning. The Home screen also displays WML applications, Favorite contact speed dial buttons, Avaya applications (World Clock and Weather), and a calculator; for more information see Special Administration for the 9670G.

Important:

You must set the system parameter AMADMIN in the 46xxsettings file for Avaya "A" Menu administration with WML applications to work.

The AvayaMenuAdmin.txt file must be a Unicode file to be properly processed by the phones. You can create a Unicode version of this file using Notepad or most text editors (select "Encoding" and "Unicode").

If WML applications are installed and the system parameter AMADMIN is set in the settings file:

- the WML applications appear in the first-level A Menu as specified in the AvayaMenuAdmin file, as shown in Figure 2.
- the first level A Menu on all 9600 Series IP Telephones except the 9670G includes a single entry (Phone Settings) that leads to a screen containing choices for Options & Settings and Network Information. For the 9670, the Home screen shows a Settings option that leads to an Options & Settings menu.
- the Phone Settings screen is essentially the current Options and Settings menu, with the addition of Network Information, as shown in Figure 3. T

If WML applications are installed and the system parameter WMLHOME is set in the settings file, the Avaya “A” Menu is identical to the pre-Release 1.2 “A” Menu, as shown in Figure 4.

If WML applications are not installed, the A Menu is essentially the same as the current Options & Settings menu, with the addition of Network Information, Log Off, and About Avaya one-X. Figure 5 provides an illustration.

There are alternatives for how the sub-applications are presented, depending on whether you have administered WML applications or not, as follows:

- Set the system parameter AMADMIN to the URL of the AvayaMenuAdmin.txt in the 46xxsettings file when you have multiple WML applications you want to display on the Avaya “A” Menu. For more information, see Main Avaya Menu with WML Applications Administered and Avaya Menu Administration With WML Applications in this chapter.
- Set the system parameter WMLHOME in the settings file for all but the 9610 when you want “Browser” to show instead of individual applications. For more information, see Main Avaya Menu with Browser (Only) Administered.
- Take no action to administer WML applications. For more information, see Main Menu – No WML Applications Administered.
- The Browser application is listed if and only if it is properly administered as specified in *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-600888). Administration also includes a non-null value for WMLHOME.

Administering Phone Settings and Options and Settings (OPSTAT and OPSTAT2)

The Options & Settings application is listed if and only if the OPSTAT value is not ***0xy***, where ***x*** and ***y*** can be any value of 0 or 1, if OPSTAT is in 3-bit form, or if and only if the value of OPSTAT is 1, if OPSTAT is in the one-digit form.

The Network Information application is listed if and only if the OPSTAT value is not ***x0y***, where ***x*** and ***y*** can be any value of 0 or 1 if OPSTAT is in 3-bit form, or in any case, if OPSTAT is in the one-digit form.

The Logout function is listed if and only if the OPSTAT value is not ***xy0,*** where ***x*** and ***y*** can be any value of 0 or 1 if OPSTAT is in 3-bit form, or if, and only if, the OPSTAT value is 1, if OPSTAT is in the one-digit form.

In general, if OPSTAT is set to forbid access to Options & Settings, changes to the user's backup file settings are ignored. This prevents someone from using the backup file as a "back door" for making changes to the settings. However, some customers centralize the customized relabeling of administered features, and want to be able to upload changes to these labels despite forbidding end users to change settings. The parameter OPSTAT2 can override the value of OPSTAT for this specific case - setting OPSTAT2 to "1" allows the telephone to accept changes to the customized labels stored in the backup file regardless of the OPSTAT value.

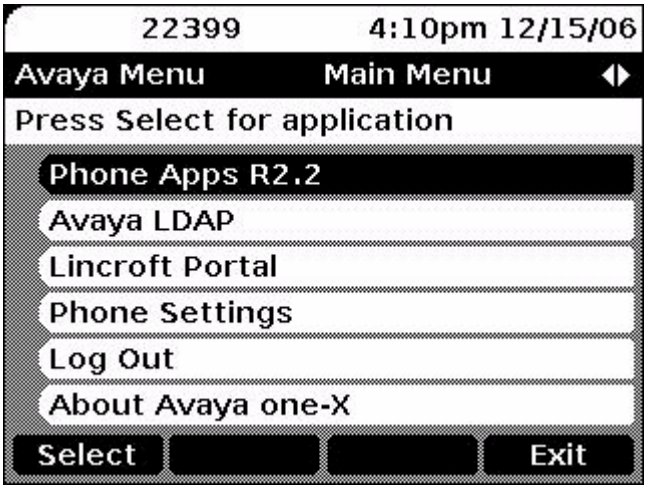
Note:

Software Release 3.0 added the system parameter OPSTAT2. Regardless of the preceding text on OPSTAT settings, if the value of OPSTAT2 has the value "1" then any customized labels in the user's backup file are uploaded and used as if the value of OPSTAT permitted this action. However, in order to restore the personalized/customized labels from the backup file to the telephone, the user needs to restart the phone by logging out and then logging back in again.

Main Avaya Menu with WML Applications Administered

Administering AMADMIN provides direct links to one or more WML applications. As Figure 2 shows, the first level Avaya Menu includes entries for three (sample) WML applications, a Phone Settings menu choice for telephone options and settings, and the telephone log out.

Figure 2: Avaya Menu with WML Applications Installed as the first three Menu options



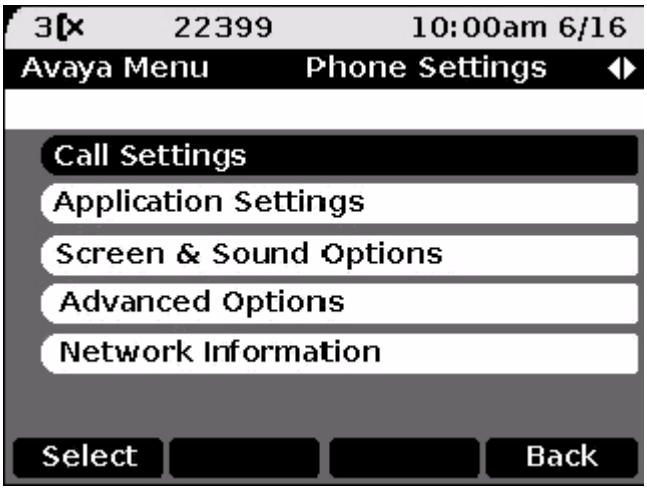
Given that at least one WML application is administered, the administrator can choose to specify the order in which not only the WML applications are presented, but also the order in which the built-in applications are presented. Any built-in applications that are not specifically

administered in the WML Administration file are automatically appended to the end of the administered list, in the following order:

- Phone Settings
- Log Out
- About Avaya one-X

Selecting (highlighting) an application and pressing **Select** or **OK** launches the application. When the Phone Settings application is listed, the Choice Indicator is also displayed on the Title Line. Pressing the Left or Right Navigation buttons displays the Phone Settings Screen. Selecting Phone Settings brings up the Phone Settings menu, shown in Figure 3.

Figure 3: Second Level Avaya Menu - Phone Settings Screen

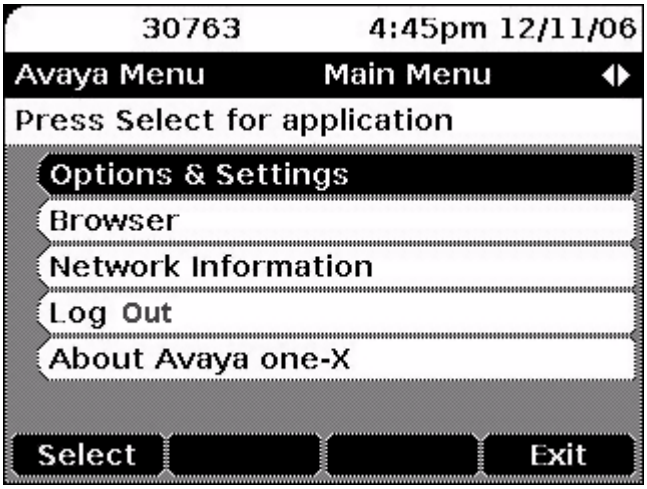


This menu is essentially the same as the current (pre-Release 1.2) Avaya Menu and provides access to user settings as well as the Log Out function.

Main Avaya Menu with Browser (Only) Administered

Setting the system parameter WMLHOME in the settings file provides a way to link to the Browser Home page by specifying a URL. Administering WMLHOME produces the Avaya “A” Menu shown in Figure 4.

Figure 4: Avaya Menu with Browser Administered using WMLHOME



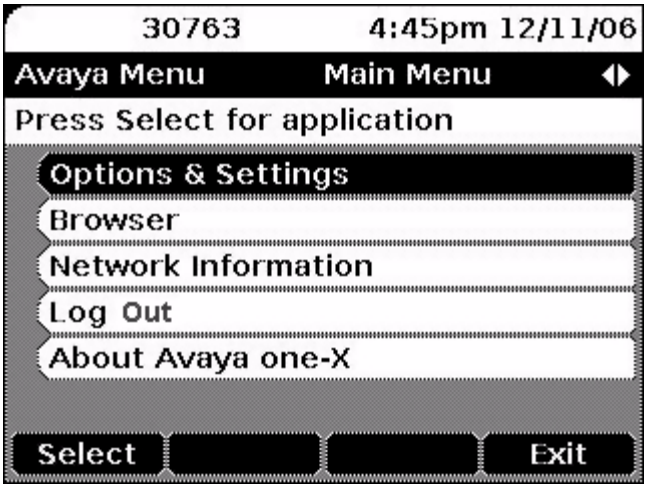
Each individual sub-application is listed left justified on an individual Application Line. From top to bottom, the sub-applications are:

- Options & Settings
- Browser
- Network Information
- Log Out
- About Avaya one-X

Main Menu – No WML Applications Administered

Figure 5 shows the Avaya Menu when no WML applications have been set up.

Figure 5: Avaya Menu With No Applications Installed



Avaya Menu Administration With WML Applications

Administer the AMADMIN parameter in the 46xxsettings file to point to a URL where the AvayaMenuAdmin.txt file resides.

Important:

The AvayaMenuAdmin.txt file must be a Unicode file to be properly processed by the phones. You can create a Unicode version of this file using Notepad or most text editors (select "Encoding" and "Unicode").

Note:

Use the AvayaMenuAdmin.txt file to specify the WML applications to appear on the 9670G Home screen.

Then specify objects for the Avaya Menu through the Avaya Menu Administration file, **AvayaMenuAdmin.txt**. Each administered object, up to the maximum of 12, must have valid, non-null parameter data:

- **AMTYPE*xx*** - One of six choices. 01=URI, 02=the local “Phone Settings” sub-application, 03=local Log Off sub-application, 04= the About Avaya one-X screen, 05=Guest Login application, 06=My Pictures application. The 9670G ignores all AMTYPE values except "1".

If the AMTYPE for an associated administered object is “01”, an additional three parameters must have valid, non-null data for the object to be properly administered:

- **AMLBL*xx*** - The label displayed to the user for this object, up to 16 UTF-16 characters, shown left-justified unless spaces precede the label value to center the label.
- **AMDATA*xx*** - A URI of up to 255 ASCII characters, without spaces.
- **AMICONxx** - For the 9670G only, any number, *N*, from 1 to 25. The 9670G will use the *Nth* icon presented in Table 20: 9670G Home Screen WML Application Icons/Labels on the Home screen in association with the administered WML application. The labels shown in Table 20 are merely suggestions; the 9670G uses the label you specify in the AMLBLxx parameter.

The ***xx*** in these three parameters is a two-digit integer from 01 to 12 inclusive, including a leading zero if applicable. If **AMTYPE*xx*** is 01, ***xx*** must be the same for each of the three parameters for an Avaya Menu entry to be displayed and associated with the administered data. If **AMTYPE*xx*** is 02, 03 or 04, any **AMLBL*xx*** or **AMDATA*xx*** data is ignored if provided.

If a given administered object has null or invalid data in any of the required associated parameters, that object is completely ignored. To list an AMTYPE01 entry on the Avaya Menu, all three associated parameters must be non-null with valid data. For example, an AMTYPE of “00” is considered invalid.

Do not administer more than nine URIs. By implication, there is no way to specify a telephone number as a TYPE (unlike the 9610).

In case of duplicate data in the settings file, the last entry is retained. For example, if two consecutive lines in the Avaya Menu Administration file are:

AMLBL01=ABCD

AMLBL01=WXYZ

then the user sees “WXYZ” as the label for the first WML application. This example assumes the rest of the administration is correct.

If no AvayaMenuAdmin.txt file is available, or if the file does not contain at least one valid type 1 (URI) object, the Release 1.0/1.1 Avaya Menu shown in Figure 5 is presented instead.

Note:

For the 9670G only, non-WML entries in the AvayaMenuAdmin.txt file are ignored.

WML Application Display on the 9670G Home Screen

Table 20 shows the icons, suggested description(s), and numbering to use to specify the WML applications you want the Home screen to display.

Table 20: 9670G Home Screen WML Application Icons/Labels

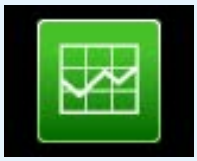
To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMBLxx)
	1	Alarm Clock/Wakeup Call
	2	Business data/Sales/Data Analysis

Table 20: 9670G Home Screen WML Application Icons/Labels

To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMBLxx)
	3	Calendar
	4	Communications
	5	Control (remote, ...)
	6	Directory
	7	Document/Folders/Notes
	8	Emergency/Assistance
	9	Food/Restaurant

Table 20: 9670G Home Screen WML Application Icons/Labels

To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMBLxx)
	10	Financial Information
	11	Front Desk
	12	Help/Site Help/Feature Help
	13	Guard Desk
	14	Information
	15	Inventory
	16	Location/Map

Table 20: 9670G Home Screen WML Application Icons/Labels

To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMBLxx)
	17	Messages
	18	Network
	19	Person/People information
	20	Security/Security Camera
	21	Tickets
	22	Valet Service

Table 20: 9670G Home Screen WML Application Icons/Labels

To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMBLxx)
	23	Video/TV
	24	Slideshow
	25	Room Service

Sample Avaya Menu Administration File Template

```
#################################################################
##                                                             ##
##     AVAYA MENU CONFIGURATION FILE TEMPLATE                  ##
#################################################################
## This file is to be used as a template for configuring
## Avaya Main Menu.  See the Avaya one-X™ Deskphone Edition for 9600 Series
##for IP Telephones Administrator Guide for details.
## Both are available on support.avaya.com
##
##Since the AMICON parameter applies only to the 9670G IP Telephone, it is not shown in the sample
below.
##
#################################################################
##
## AMLBLxx=Label   up to 16 unicode characters
##
## AMTYPExx=Type   1=WML-Application;
##           2=local Phone Settings
##               3=local LogOff Application
##               4=local About Avaya Screen
##               5=Guest Login
##               6=My Pictures
##
## AMDATAxx        URI of up to 255 ASCII-characters
##               e.g. http://yy.yy.yy.yy/*.wml
##
## The tags AMLBLxx and AMDATAxx are only used if
## AMTYPExx = 1
##
## Multiple definitions of local applications (Type 2.4)
## will be suppressed. The last tag is valid.
##
## xx describes the sequence in A-Menu and is valid
## from 01 to 12
##
##


##AMTYPE01=
##AMLBL01=
```

##AMDATA01=

##AMTYPE02=
##AMLBL02=
##AMDATA02=
##AMTYPE03=
##AMLBL03=
##AMDATA03=

##AMTYPE04=
##AMLBL04=
##AMDATA04=

##AMTYPE05=
##AMLBL05=
##AMDATA05=

##AMTYPE06=
##AMLBL06=
##AMDATA06=

##AMTYPE07=
##AMLBL07=
##AMDATA07=

##AMTYPE08=
##AMLBL08=
##AMDATA08=

##AMTYPE09=
##AMLBL09=
##AMDATA09=

##AMTYPE10=
##AMLBL10=
##AMDATA10=

##AMTYPE11=
##AMLBL11=
##AMDATA11=

##AMTYPE12=
##AMLBL12=
##AMDATA12=

Guest User Administration

A “guest user” is anyone who logs into a 9600 Series IP Telephone that is not his or her primary phone at the user’s home location. This could mean that the guest user can log into a telephone that is across the country from the home location or one in the office adjacent to the home office. You administer permission for guest login by setting the system parameter GUESTLOGINSTAT to “1” (permitted), which in turn displays the Guest Login option on the Avaya “A” Menu. Other related parameters you can administer are GUESTDURATION (which can be overridden by a different, user-entered duration during login) and GUESTWARNING. All parameters are described in Table 18 and Table 11.

Timer Operation for the 9620/9620L/9620C, 9630/9630G, 9640/9640G, 9650/9650C and 9670G

When the idle timer in the telephone expires you can administer the telephone to turn off the backlight, put up a screen saver, and/or show a Web page while the telephone is idle. However, Avaya does not recommend setting all of these values on the same telephone. Avaya does recommend, for instance, that you set a lobby phone to go to a Web page when it is idle and to set a desk phone to go to the screen saver and/or turn off the backlight when idle.

The related system parameters and their default values, further described in Table 11: 9600 Series IP Telephone Customizable System Parameters, are:

- WMLIDLETIME = 10 minutes
- BAKLIGHTOFF = 120 minutes
- SCREENSAVERON = 240 minutes
- WMLIDLEURI = null

WMLIDLEURI is expected to be specified only for phones in public areas through the use of a GROUP parameter.

Table 21: Idle Timer Settings and Results

Shortest Timer	Middle Timer	Longest Timer	Operation
WMLIDLETIME and WMLIDLEURI are null	BAKLIGHTOFF is non-zero	SCREENSAVERON is non-zero	Default operation: After BAKLIGHTOFF minutes, the backlight turns off. After (SCREENSAVERON – BAKLIGHTOFF) additional minutes, the screen saver is displayed. WMLIDLETIME has no effect.
WMLIDLETIME and WMLIDLEURI are null	SCREENSAVERON is non-zero	BAKLIGHTOFF is non-zero	After SCREENSAVERON minutes, the screen saver is displayed. After (BAKLIGHTOFF – SCREENSAVERON) additional minutes, the backlight turns off.
WMLIDLETIME and WMLIDLEURI are non-null	BAKLIGHTOFF is non-zero	SCREENSAVERON is non-zero	Every WMLIDLETIME minutes, a GET is sent for WMLIDLEURI, and the browser is displayed. The Web page may contain its own timer to cycle through additional Web pages. For all phones except 9670G - The backlight is turned off after the specified time and the screen saver is displayed based on the SCREENSAVERON value. For 9670G only - the backlight is set to low power mode rather than turned off and the screen saver is displayed based on the SCREENSAVERON value.

Note:

The 9610 IP Telephone uses the IDLEAPP value in the 9610data.txt file instead of WMLIDLEURI in the settings file. For more information, see Special Administration for the 9610 on page 145 and 9610 Backup/Restore on page 132.

Note:

The Backlight Off icon allows the end users to bypass the timers in Table 21 and turn the backlight off automatically. You can administer the Backlight Off icon on a 9600 Series IP Telephone softkey as described in Administering Features on Softkeys. The backlight for any adjunct button module will follow the behavior of the backlight of the telephone to which the button module is attached.

Requirements for USB Devices

A USB device can be used to carry information to support the following usage profiles:

- Mobility/Visiting User: The USB memory stick carries login credentials, contacts and/or digital pictures. Inserting a USB device will cause the phone to register with a login profile, allowing any 9600 Series IP Telephone to become a personalized extension.
- Deskphone Personalization: A USB memory stick supports import/export of contacts to/from a 9600 Series IP Telephone and/or display of digital pictures.

Users and administrators can use the *Avaya one-X™ Deskphone USB Companion,* a PC-based USB management tool that converts Microsoft Office Outlook contacts to a format usable by 9600 Series IP Telephones, and provides an easy way to format other files, like digital pictures that will be used as screensavers. This pc-based tool is available on the Avaya support Web site.

USB File/Device Support

Only FAT or FAT32 file systems are currently supported. The following are not currently supported:

- USB drives with NTFS file systems are not supported.
- USB devices with multiple partitions or multiple LUNS are not supported.
- U3 USB devices are not supported.

Contacts File Format for USB Devices

As of software Release 2.0, Contacts lists can be imported or exported to or from all 9600 Series IP Telephones (except the 9610) via a USB device like a Flash drive or memory stick. The telephone user guide provides detailed information on this capability.

Contact files merged or written to the phone's Contacts list must be in a specific format. The user guides advise end users of two ways to ensure that a Contact list is formatted properly.

The rest of this section documents the 9xxxContacts.txt file requirements. Use this information as a guide to export contacts from Outlook and other similar software applications without using the Avaya one-X™ Deskphone USB Companion tool.

The contacts file must be a little-endian Unicode text file. That is, each ‘character’ in the file is a 16-bit integer value, stored least significant byte first. The first two bytes of the file are a Byte Order Mark which must be FF followed by FE (hexadecimal). The file name must be “9xxxContacts.txt” (without the quotes).

Each contact entry consists of a single line, terminated by <CR><LF> (Carriage Return, 000D hex, and Line Feed, 000A hex). An entry contains 1 name, 1 to 3 phone numbers, and 0 to 3 types. Separate the fields within each contact entry with one or more tabs.

The detailed contact entry format is:

<name><tab><number1><tab><type1><tab><number2><tab><type2><tab><number3><tab> <type3><CR><LF>

Name and Number fields - can start and end with a double quote character ["]). The name and number1 are required, and each must be at least one character (not counting quotes). Limit names and phone numbers to 20 characters for the name, 30 for the numbers. Values are truncated if they exceed these maximum sizes.

Types - must be 3 characters, starting and ending with a slash ‘/’ character, with a digit character 0 to 3 in between; e.g. “/1/”. Leading and/or trailing spaces are ignored for type fields. The Types are 0 for General, 1 for Work, 2 for Mobile, and 3 for Home. Types are optional and missing types default to 0 (General).

Lines may be at most 255 Unicode characters long, including the <CR><LF>. Blank lines, including lines consisting only of spaces and/or tabs, are ignored. A field other than the first that consists of only spaces is ignored.

Because types can be omitted, if the potential type field is more than 3 characters or does not start and end with a slash, it is considered the next number field, if any (e.g. “/1” and “/02/” would be considered numbers).

Entries are invalid if:

- the name is null (a non-blank line starts with tab or with “” followed by tab).
- there is no number1 field.
- any number field is null (for example, just “” for number2).
- a potential type field contains an invalid digit (not 0, 1, 2, or 3) or consists of “/” or “//”.
- more than three numbers are provided.
- the entry contains more types than numbers.

The Windows™ XP Notepad program allows Unicode text files to be created and edited. Use the Save As dialog to set the file “Encoding” to “Unicode.”

USB Login Setup

As of software Release 3.0, users can be allowed to log in to their call servers via a USB Login profile. As the administrator, you enable this feature by allowing the parameter USBLOGINSTAT in the settings file to remain at the default value of "1" or you can disable this feature by changing the value to "0". The advantage of having USB login is that users can go anywhere in the world having sufficient network data connectivity, plug the USB device into a 9600 Series IP

Telephone running software Release 3.0 or later and log into their home call server using their own extension and get all their home administered features.

You can use *Avaya one-X™ Deskphone USB Companion*, the Avaya PC-based USB management tool, to create the USB login profile and specify whether the login password should be encrypted or stored in the clear. For more information on this tool, see the Avaya support Web site, http://www.avaya.com/support.

Note:

When users log in via the USB Login feature, the telephone does not attempt to access the backup file as normal, so normal user-specified data such as Options, or Call Log entries are not available. The reason is that if the user is in a different environment from the usual office the telephone would attempt to access the local backup file server instead of the remote (home) file server and could obtain a different backup file than that of the user.

Additionally, the only contacts a user has access to when registered via USB Login are the contacts available on the USB device (properly formatted as a 9xxxContacts.txt file using the Avaya USB tool or another method).

USB Pictures

As of Software Release 3.0, one or more pictures from a USB flash drive device can be used as screen savers. The USB device may contain any number of .jpg or .jpeg files that can be used in place of a default or custom screen saver(s). If multiple files are provided, the telephone will present each picture in order, based on the order the pictures were saved, changing to the next image after the number of seconds specified by the timer parameter, which has a default of 5 seconds. These pictures also be viewed directly by using the "My Pictures" option on the Avaya "A" Menu or on the 9670G Home screen.

Users and administrators can use the *Avaya one-X™ Deskphone USB Companion* to format digital pictures that will be used as screensavers. This pc-based tool is available on the Avaya support Web site.

If you want to set up digital picture files manually without using the *Avaya one-X™ Deskphone USB Companion*, follow these instructions:

1. Create a "\Pictures" directory on the USB device.
2. Add one or more images with an extension of *.jpeg or *.jpg, and with a valid JPEG format to the pictures directory. The images should not exceed the pixel sizes below for the respective telephone model. Color phones such as the 9620C, 9640, and 9650G display a better image quality than those 9600 Series IP Telephones that do not have color displays:
   - For 9620 IP Telephones, use 320 x 160.
   - For all other 9600 Series IP Telephone models, use 320 x 240.

Note:

Images that are too large to be displayed on the phone will not be displayed; in this case, the default screensaver image will be shown instead.

The 9610 IP Telephone does not have a USB interface and therefore cannot display digital images as screensavers.

Note:

The screensaver will start automatically when the phone is idle for the time specified in the SCREENSAVERON parameter (default is 240 minutes). In practice, it is useful to reduce this time in order to use the USB Pictures feature.

To disable USB picture functionality, set the SCREENSAVERON parameter to "0" in the settings file.

Chapter 9: Administering Specific 9600 Series IP Telephones

Introduction

Some 9600 IP Telephone models may require that you administer additional features or have special administrative requirements. For example, the 9610 IP Telephone is a one-line telephone designed as a courtesy, or walk-up, telephone. The 9610 is not full-featured like other 9600 IP Series Telephones, with just a Contacts application, but additional features like WML applications and a Directory can be administered for a 9610.

This chapter provides additional or alternate administration details for specific telephone models.

Special Administration for the 9610 IP Telephone

General Functionality

Because the 9610 is a single line phone, the user cannot transfer or conference calls, or put an active call on hold.

The 9610 does not have a phone screen like other 9600 Series IP Telephones. There are two application buttons - **Start** and **Contacts**. There are no “A” or Call Log buttons, Speaker or Mute buttons. The Web browser application is supported.

The **Main Menu (MM)** on the Start screen is an administrable list of “objects” from which a user can select a new application that is either local to the telephone or on an external server, or an outgoing call. Underlying Main Menu content administration directs the telephone to take action applicable to the given selection. The default Main Menu consists of Contacts and Directory, assuming they have been appropriately administered. The Main Menu displays when the telephone first powers up or resets.

The **Contacts Application** provides functionality similar to the other models but only to launch a call to a contact. Contacts cannot be edited, deleted or added.

The **Idle Application** displays when both a Web Idle Timer and the Idle application have been administered and the timer expires. For example, if the Idle application has been set to “Contacts,” when the Web Idle Timer expires the 9610 display changes to the Contacts application. The Idle application is either one of the existing local applications (Menu or Directory) or a URL, depending on the contents of IDLEAPP.

Key 9610 Administration Concepts

Each 9610 seeks a backup/restore file which contains essential administration data in its user interface that enables different capabilities to walk-up users. The backup file concept is common to all phones, but in the case of the 9610, must be created by an administrator to specify the required behavior of the telephone to walk-up users. Backup and retrieval for the 9610 is covered in more detail in 9610 Backup/Restore on page 132.

A group of 9610 phones can share a common backup file, or individual 9610 IP Telephones can have individual customized backup files.

Backup files must be created in an editor. There is no capability to store a current configuration from the phone to a backup file as there is for other 9600 Series models.

Within the backup file format, the configuration is split into three portions corresponding to the applications mentioned in General Functionality:

- Main Menu administration as described on page 170.
- Contacts administration as described on page 171.
- Idle administration as described on page 171.

Create a generic backup/restore file named "9610data.txt" that can be used as a default to provide basic functionality and serve as a template for any customized 9610 extensions. Create a backup/restore file named "Ext#_9610data.txt" for the specific extension you want to customize.

See the Avaya support site http://support.avaya.com to download a 9610 backup file example. A sample file also appears on Sample 9610data.txt File on page 174.

Note:

Like other telephone models, the 9610 looks for a 46xxsettings file at startup. In the 46xxsettings file, the system parameter BRURI must be set to the URI where the 9610data.txt file is located. This consists of the HTTP server IP Address and (optional) directory.

If the telephone cannot find the 9610data.txt file or if that file does not exist, the screen displays the default Main Menu (Contacts and Directory).

Backup File Format

Use a text editor to create the 9610 backup file. Characters are assumed to be coded in UTF-16 LE (little-endian), with Byte Order Mark (BOM) for LE (0xFFFE)), with each item on a separate line terminated by" <CR><LF>" (000D 000A in UTF-16) characters.

The generic format for data values is: ***name=value***.

The format for a Main Menu entry is:

MMLBL*xx=entry label*

MMTYPE*xx=entry type*

MMDATA*xx=entry data*

The format for a Contacts entry is:

CONLABEL*xxx=entry label*

CONDATA*xxx=entry data*

Other parameters that have meaning in a 9610 backup file are:

IDLEAPP

LISTAPP

When retrieving data, the following applies:

- If the BOM is not 0xFFFE, the entire file is rejected and the retrieval is considered to have failed.
- All identifiers (for example, names) are interpreted in a case-insensitive manner.
- The case of parameter values and Contacts names and numbers is preserved.
- Spaces preceding, within, or following a name or value are treated as part of that entity.
- <CR> and <LF> are interpreted as line termination characters.
- Blank lines are ignored.
- If an identifier is not recognized or is invalid, the entire line is ignored.
- If an identifier is valid but the data itself is invalid or incomplete, the line is ignored. The determination of what constitutes a valid value for each data element is specified in the individual requirements in this document.
- If more than one line contains a value for a parameter or Contacts entry, the last value read is used. Hence, new values overwrite previous values as lines are read from the file. In all other cases, the order of the lines in the file does not matter.

The success of the retrieval process requires the telephone to obtain the backup file and to successfully store valid data. The existence of invalid data does **not** constitute a failed retrieval.

Main Menu (MM) Administration

Use the 46xxsettings file to set the system parameter BRURI to point to the URI where the 9610 backup/restore file (9610data.txt) resides. Then specify objects for the Main Menu via the “9610data.txt” backup file.

Note:

The 9610 will not display a Main Menu unless you set BRURI to point to the 9610data.txt file and specify Main Menu objects.

Each administered object, up to the maximum of 10, must have valid, non-null data in each of the three parameters as indicated:

- **MMLBL*xx*** - the label displayed to the user for this object, up to 16 characters.
- **MMTYPE*xx*** - one of four choices: 01=URI, 02=telephone number, 03=local Contacts application, 04=local Directory application.
- **MMDATA*xx*** - the data used depends on the value of MMTYPExx:
  - a URI, if MMTYPE is “01,”
  - a dialable string if MMTYPE is “02,”
  - the English word “Contacts” if MMTYPE is “03,” and
  - the English word “Directory” if MMTYPE is “04.”

Note:

If administered as a URI, MMDATAxx is up to 255 ASCII characters in length.

In these parameters, ***xx*** is a two-digit integer from 01 to 10 inclusive, including a leading zero if applicable. If MMTYPE is 01 or 02, ***xx*** must be the same for each of the three parameters for a Main Menu entry to be displayed and associated with the administered data. If MMTYPE is 03 or 04, ***xx*** must be the same as a corresponding MMLBL item for a Main Menu entry to be displayed, but no MMDATA need be assigned. Any MMDATA assigned to that ***xx*** entry is ignored.

If a given administered object has null or invalid data in any of the required associated parameters, that object is completely ignored. Therefore for a MMTYPE 01 or 02 entry to be listed on the Main Menu, all three associated parameters must be non-null with valid data. An MMTYPExx of “00” is considered invalid.

The default values for Main Menu (MM) objects are:

Parameter	Default Value
MMLBL01	Contacts (automatically translated into the user interface language).
MMTYPE01	3 (Local Contacts application).
MMDATA01	Contacts (English only)
MMLBL02	Directory (automatically translated into the user interface language).
MMTYPE02	4 (Local Directory application).
MMDATA02	Directory (English only).

The default “Directory” will appear as the first Main Menu object whenever it is not administered in the Main Menu, if there is no 9610 backup file, or if retrieval of the backup file fails.

The DATA terms “Contacts” and “Directory” are always administered in English, and are independent of the user interface (UI) language. The administrator can create labels for the local applications in the UI language if desired. The administrator can use, for example, “Contacts” for a browser-based application, and “List” for the local Contacts application. Instead, the term used presents the appropriate local application, which does present the UI in the user’s language.

The Main Menu allows up to 10 administrable objects including the two local application objects, Contacts, and Directory so that the total number of items fit on two screens.

Contacts Application Administration

The administrator populates the Contacts Application via the backup file. Each administered object, up to the maximum of 250, must have valid, non-null, data in both of the parameters as indicated:

CONLABEL*xxx* (the label displayed to the user for this object)

CONDATA*xxx*

In the list of parameters above, ***xxx*** is a three-digit integer from 001 to 250 inclusive. To display and associate with the administered data, the three-digit integer must be the same for both parameters. The ***xxx*** value includes leading zeroes as applicable.

If a given administered object has null or invalid data in any of the two associated parameters, that object is completely ignored. Hence, to be listed in the Contacts application, both associated parameters must be valid and non-null.

CONLABEL*xxx* data maps to the corresponding ENTRY_NAME. **CONDATA*xxx*** maps to the corresponding ENTRY_NUMBER_1.

All contacts are sorted in alphanumeric order on the Phone screen regardless of the order put in the backup/restore file.

The 9610 Idle Application, WMLIDLETIME, SCREENSAVERON, IDLEAPP, and WMLSMALL

The 9610 IP Telephone can present a variety of behaviors if the telephone is left idle for a period of time.

WMLIDLETIME - This parameter (set in the 46xxsettings file, if administered) specifies the number of minutes the phone must be idle before an Idle Application specified by IDLEAPP can be presented on the display.

SCREENSAVERON - This parameter (set in the 46xxsettings file, if administered) specifies the number of minutes the phone must be idle before the Avaya Screen Saver can be presented on the screen.

Note:

In the current firmware version, it is not advisable to use both WMLIDLETIME and SCREENSAVERON. For example, one value should be set to 999 and the other to some nominal time, perhaps 30 minutes.

WMLSMALL - This parameter (set in the 46xxsettings file, if administered) is required to be non-null for WML links specified in the Main Menu to be displayed. Set this value to a valid URL, and under certain circumstances, it will become the Idle Application displayed on the phone.

IDLEAPP - If the IDLEAPP parameter is administered as " " (Null, the default value), when the Web Idle Timer expires, the URL that WMLSMALL points to is presented, if WMLSMALL is administered. If both IDLEAPP and WMLSMALL are null, the 9610 displays the Avaya one-X Screen.

If IDLEAPP is administered as:

- **Menu** - when the Web Idle Timer expires, the telephone displays the Main Menu application if the Main Menu is not empty. If the Main Menu is empty, the Avaya Screen displays instead.
- **Directory** - when the Web Idle Timer expires, the telephone displays the Directory application. If a Directory does not exist, the telephone displays the Avaya Screen.
- **Contacts and LISTAPP is non-null** - when the Web Idle Timer expires, the telephone launches the Contacts application.
- **Contacts and LISTAPP is null** - and the local Contacts application is not empty when the Web Idle Timer expires, the telephone launches the local Contacts application. If the local Contacts application is empty, the telephone displays the Avaya Screen.

  Note:

  The terms “Menu,” “Contacts,” and “Directory” are always administered in English. The terms are independent of the user interface language, since the telephone does not directly present the value of IDLEAPP to the user. Instead, the term is used to present the appropriate local application, which does present the user interface in the user’s language.

If IDLEAPP is administered as “Directory”, and the Directory application is the ACP-based Integrated Directory, then the telephone will have to reinstate the application approximately every minute, since the feature automatically times out after that interval.

If the screen saver is displayed, the Idle Application is not visible until the screen saver is removed. The screen saver is removed when the user goes off-hook, presses a button, or the telephone receives an incoming call.

For example:

- if an IDLEAPP display is desired when the telephone has been idle for 30 minutes, Avaya recommends that IDLEAPP be administered as non-null, that WMLIDLETIME be set to “30” and SCREENSAVERON be set to “999.”
- If a WMLSMALL URL display is desired when the phone has been idle for 30 minutes, Avaya recommends that IDLEAPP be administered as " " (null), that WMLIDLETIME be set to “30,” that SCREENSAVERON be set to “999,” and that WMLSMALL be administered as a valid URL.
- To display the Avaya Screen Saver after 30 minutes of telephone idle time, set IDLEAPP to " " (null), set WMLIDLETIME to “999,” set WMLSMALL as desired (with a URL if Main Menu WML links are to be displayed, or null if not), and set SCREENSAVERON to “30.”

See Sample 9610data.txt File, Sample idle.wml File, and Sample hotel.wml File for examples of generic files to use as templates. Also see the Avaya 9600 Series IP Telephones support Web site for a downloadable example of typical 9610 setup files.

9610 Craft Procedures

Unlike the other 9600 Series IP Telephones, press the **Contact** button twice instead of pressing **Mute** to access local procedures.

Troubleshooting a 9610 IP Telephone

- If the Directory functionality is not present, make sure that you administer “Directory,” “Next,” and “Call-disp” (the latter which shows as “Make call” on the telephone) on the CM station form in the first six call appearances/feature buttons. (Applies to pre-CM4.0 only.)
- Any call appearances/features administered beyond the first six call appearances/feature buttons will be ignored. (Applies to pre-CM4.0 only.)
- If calls cannot be received on the 9610, check the station administration for a "y" in the "Restrict Last Appearance" field. Change to "n" to allow incoming calls.
- If the “Ext#_9610data.txt" is not set up, the phone will default to the "9610data.txt" file.
- If the "9610data.txt" file is not set up, the telephone displays the message "Restore Failed." and the default Avaya start screen. In this case, even if CM Directory is administered, the start screen appears and the Directory application will not be available.
- If “`Restore Failed`” appears on the screen when you bring up a 9610, this indicates the telephone could not find or load the backup file.
  - Check folder and file availability and permissions.
  - Check to be sure the filename matches the required conventions for individual extensions or generic backup for all 9610 IP Telephones.
  - Check to be sure the 46xxsettings.txt file has a “Set BRURI http://xxx.xxx.xxx.xxx” entry, where “xxx.xxx.xxx.xxx” is the IP Address of the HTTP server where the 9610data.txt file is stored.
  - Check to be sure there is a byte order mark (BOM) in the 9610data.txt file. The BOM is generated when the 9610data.txt file is saved in Unicode format.
- The WMLSMALL parameter must be non-null for Main Menu WML links to be displayed.

Sample 9610data.txt File

```
##
## THE FOLLOWING "CON" SECTION IS
## THE DEFAULT 9610 "CONTACTS LIST"
## AND MAY BE POPULATED WITH REAL
## NAMES AND TELEPHONE NUMBERS
## OR EXTENSIONS FOR YOUR COMPANY.
## THE ITEMS WILL NOT APPEAR IN THE
## ORDER OF THE LABEL NUMBERS BUT
## RATHER, IN ASCII ALPHA ORDER. THE
## CONTACTS LIST MAY BE SELECTED
## USING THE 9610's RIGHT SIDE (BOOK)
## "CONTACTS" BUTTON. THE "CON"
## MENU WILL SCROLL IF MORE THAN 6
## LABEL GROUPS ARE CONFIGURED.
## NOTE: "+" BELOW INDICATES NON WORKING
## TELEPHONE NUMBERS.
##
CONLABEL001=c: Security+
CONDATA001=12345
CONLABEL002=b: Building Svc+
CONDATA002=9155555555555
CONLABEL003=d: Help+
CONDATA003=9155555555555
CONLABEL004=a: Audix+
CONDATA004=12345
CONLABEL005=9610-DEMO-ONLY+
CONDATA005=DUMMY
CONLABEL006=+NOT WORKING#'s
CONDATA006=DUMMY

##
## THE FOLLOWING ""MM" SECTION IS
## THE DEFAULT "MAIN MENU" AND
```

```
## NORMALLY APPEARS FOLLOWING
## A 9610 REBOOT OR POWER UP.
## THE ""MM" GROUPS MAY BE
## REPLACED WITH WML LINKS OR
## TELEPHONE NUMBERS APPROPRIATE
## TO YOUR INSTALLATION, INCLUDING
## THE IP ADDRESS OF YOUR FILE
## SERVER AND WML PATH. NOTE THAT
## WMLSMALL MUST BE A VALID URL FOR
## WML LINKS TO DISPLAY IN THIS MENU.
## THE "MM" MENU WILL SCROLL IF MORE
## THAN 6 LABEL GROUPS ARE CONFIGURED.
##
MMLBL01=ABOUT-9610
MMTYPE01=1
MMDATA01=http://135.8.60.18/WML/about.wml
MMLBL02=MyCo Today
MMTYPE02=1
MMDATA02=http://135.8.60.18/WML/index.wml
MMLBL03=MyCo Directory
MMTYPE03=4
MMDATA03=Directory
MMLBL04=Visitor Info
MMTYPE04=1
MMDATA04=http://135.8.60.18/WML/visit_lz.wml
MMLBL05=Printer Trouble
MMTYPE05=1
MMDATA05=http://135.8.60.18/WML/printer-rooms.wml
MMLBL06=Call Jack+
MMTYPE06=2
MMDATA06=32099
```

Note that the information entered into the backup/restore file is what controls the 9610 Main Menu. The references within the files are to ".wml" files, which are text Web pages and an example is provided for illustration only. **The content of these files must be customized for specific phones/sites.** The wml files can be placed at the root level or buried in a lower level directory if desired. Modify the Backup/Restore and 46xxsettings file references accordingly.

Sample idle.wml File

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN" "http://
  www.wapforum.org/DTD/wml13.dtd">
<wml>
      <card id="splash" title=" ">
       <p align="center">
        <img src="img/one-X_w150_h70.wbmp" alt="Avaya one-X(TM)"/>
       </p>
     </card>
</wml>
```

Sample hotel.wml File

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN"
         "http://www.wapforum.org/DTD/wml13.dtd">
<wml>
  <card id="hotel" title="Hotels">
    <p><a href="hotels/marriott_courtyard.wml">Marriott Courtyard</
      a></p>
    <p><a href="hotels/extended_stay.wml">Extended Stay</a></p>
    <p><a href="hotels/molly_pitcher.wml">Molly Pitcher</a></p>
       <p><a href="hotels/oyster_point.wml">Oyster Point</a></p>
       <p><a href="hotels/holiday_inn.wml">Holiday Inn</a></p>
  <do type="prev" label="Back"><prev/></do>
  </card>
</wml>
```

Appendix A: Glossary of Terms

802.1D 802.1Q	802.1Q defines a layer 2 frame structure that supports VLAN identification and a QoS mechanism usually referred to as 802.1D.
802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. Applicable 9600 Series IP telephones support IEEE 802.1X for pass-through and for Supplicant operation with the EAP-MD5 authentication method.
ARP	Address Resolution Protocol, used, for example, to verify that the IP Address provided by the DHCP server is not in use by another IP telephone.
CA	Certificate Authority; the entity which issues digital certificates for use by other parties.
CELP	Code-excited linear-predictive. Voice compression requiring only 16 kbps of bandwidth.
CLAN	Control LAN, type of Gatekeeper circuit pack.
CNA	Converged Network Analyzer, an Avaya product to test and analyze network performance.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.
Diffie -Hellman key exchange	A key agreement algorithm based on the use of two public parameters p and g that may be used by all users in a system. Parameter p is a prime number and parameter g (usually called a generator) is an integer less than p.
DH Group	A number that determines the public parameters used by the Diffie-Hellman key exchange. To successfully establish a shared secret key, the same DH group must be used by both parties.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
Digital Certificate	The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by a trusted third party known as a "Certificate Authority" (CA) such as VeriSign (www.verisign.com). The CA verifies that a public key belongs to a specific company or individual (the "Subject"), and the validation process it goes through to determine if the subject is who it claims to be depends on the level of certification and the CA itself.

Digital Signature	A digital signature is an encrypted digest of the file (message, document, driver, program) being signed. The digest is computed from the contents of the file by a one-way hash function such as MD5 or SHA-1 and then encrypted with the private part of a public/private key pair. To prove that the file was not tampered with, the recipient uses the public key to decrypt the signature back into the original digest, recomputes a new digest from the transmitted file and compares the two to see if they match. If they do, the file has not been altered in transit by an attacker.
DNS	Domain Name System, an IETF standard for ASCII strings to represent IP Addresses. The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP Addresses. Avaya 9600 Series IP Telephones can use DNS to resolve names into IP Addresses. In DHCP, TFTP, and HTTP files, DNS names can be used wherever IP Addresses were available as long as a valid DNS server is identified first.
Gatekeeper	H.323 application that performs essential control, administrative, and managerial functions in the media server. Sometimes called CLAN in Avaya documents.
H.323	A TCP/IP-based protocol for VoIP signaling.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	A secure version of HTTP.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.
IKE	Internet Key Exchange Protocol, RFC 2409, which has been obsoleted by IKEv2 in RFC 4306.
IPsec	A security mechanism for IP that provides encryption, integrity assurance, and authentication of data.
ISAKMP	Internet Security Association and Key Management Protocol, RFC 2408, which has been obsoleted by IKEv2 in RFC 4306, defines the procedures for authenticating a communicating peer, creation and management of security associations, key generation techniques, and threat mitigation e.g. Denial of service and Replay Attacks. ISAKMP defines two phases of negotiation. During Phase 1 negotiation, two entities establish an ISAKMP SA, which is used to protect Phase 2 negotiations, in which SAs are established for other protocols.
LAN	Local Area Network.
LLDP	Link Layer Discovery Protocol. All IP telephones with an Ethernet interface support the transmission and reception of LLDP frames on the Ethernet line interface in accordance with IEEE standard 802.1AB.
MAC	Media Access Control, ID of an endpoint.

Media Channel Encryption	Encryption of the audio information exchanged between the IP telephone and the call server or far end telephone.
NAPT	Network Address Port Translation.
NAT	Network Address Translation, a mechanism by which IP addresses are mapped from one address space to another, and in which UDP and TCP port numbers may be remapped to allow multiple devices to share the same IP address without port number conflicts.
OPS	Off-PBX Station.
PHP	Hypertext Preprocessor, software used to assist in the format and display of Web pages.
PSTN	Public Switched Telephone Network, the network used for traditional telephony.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks.
Refresh/ Rekey	Use IKE to create a new SA with a new SPI.
RSA	Rivest-Shamir-Adleman; a highly secure asymmetric cryptography method developed by RSA Security, Inc. that uses a public/private key pair. The private key is kept secret by the owner and the public key is published, usually in a digital certificate. Data is encrypted using the recipient's public key, which can only be decrypted by the recipient's private key. RSA is very computation intensive, thus it is often used to encrypt a symmetric session key that is then used by a less computationally-intensive algorithm to encrypt protocol data during a "session". RSA can also be used for authentication by creating a digital signature, for which the sender's private key is used for encryption, and the sender's public key is used for decryption.
RSVP	Resource ReSerVation Protocol, used by hosts to request resource reservations throughout a network.
RTCP	RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service.
RTP	Real-time Transport Protocol. Provides end-to-end services for real-time data such as voice over IP.
SA	Security Association, a security protocol (e.g., IPSEC, TLS) and a specific set of parameters that completely define the services and mechanism necessary to protect security at that security protocol location. These parameters can include algorithm identifiers, modes, cryptographic keys, etc. The SA is referred to by its associated security protocol (for example "ISAKMP SA", "ESP SA", "TLS SA").
SCEP	Simple Certificate Enrollment Protocol, used to obtain a unique digital certificate.
SDP	Session Description Protocol. A well-defined format for conveying sufficient information to discover and participate in a multimedia session.

Signaling Channel Encryption	Encryption of the signaling protocol exchanged between the IP telephone and the call server. Signaling channel encryption provides additional security to the security provided by media channel encryption.
SIP	Session Initiation Protocol. An alternative to H.323 for VoIP signaling. This protocol is not applicable to 9600 Series IP Telephones.
SNTP	Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet.
SOHO	Small Office Home Office. The environment for which a virtual private network (VPN) would be administered.
SPD	Security Policy Database. Specifies the policies that determine the disposition of all IP traffic inbound or outbound from a host or security gateway IPsec implementation.
SPI	Security Parameter Index. An identifier for a Security Association, relative to some security protocol. Each security protocol has its own "SPI-space".
SRTCP	Secure Real-time Transport Control Protocol.
SRTP	Secure Real-time Transport Protocol.
system -specific	Specific to a particular type of call server, e.g., Avaya Communication Manager (CM) or SIP Enablement Services (SES). "System-specific signaling" refers to messages specific to the signaling protocol used by the system, e.g., H.323 and/or CCMS messages used by CM and IP Office, or SIP messages (possibly including system-specific headers) used by SES. "System-specific procedures" refers to procedures in telephone software that are specific to the call server with which the software is intended to be used.
TCP/IP	Transmission Control Protocol/Internet Protocol, a network-layer protocol used on LANs and internets.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP telephones.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications.
TLV	Type-Length-Value elements transmitted and received as part of Link Layer Discovery Protocol (LLDP).
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
Unnamed Registration	Registration with Avaya Communication Manager by an IP telephone with no extension. Allows limited outgoing calling.
URI & URL	Uniform Resource Identifier and Uniform Resource Locator. Names for the strings used to reference resources on the Internet (for example, HTTP://....). URI is the newer term.
VLAN	Virtual LAN.

VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.
VPN	Virtual Private Network; a private network constructed across a public network such as the Internet. A VPN can be made secure, even though it is using existing Internet connections to carry data communication. Security measures involve encrypting data before sending it across the Internet and decrypting the data at the other end. An additional level of security can be added by encrypting the originating and receiving network address.
WML	Wireless Markup Language, used by the 9600 Series IP Telephone Web Browser to communicate with WML servers.

5 of 5

Appendix B: Related Documentation

IETF Documents

IETF documents provide standards relevant to IP Telephony and are available for free from the IETF Web site: http://www.ietf.org/rfc.html.

ITU Documents

Access the ITU Web site for more information about ITU guidelines and documents, available for a fee from the ITU Web site: http://www.itu.int.

ISO/IEC, ANSI/IEEE Documents

Access the ISO/IEC standards Web site for more information about IP Telephony standards, guidelines, and published documents: http://www.iec.ch.

Appendix C: Sample Administration Forms

Use the sample screens that follow as guidelines for telephone setup.

Figure 6: Station Form - Basic Telephone Information

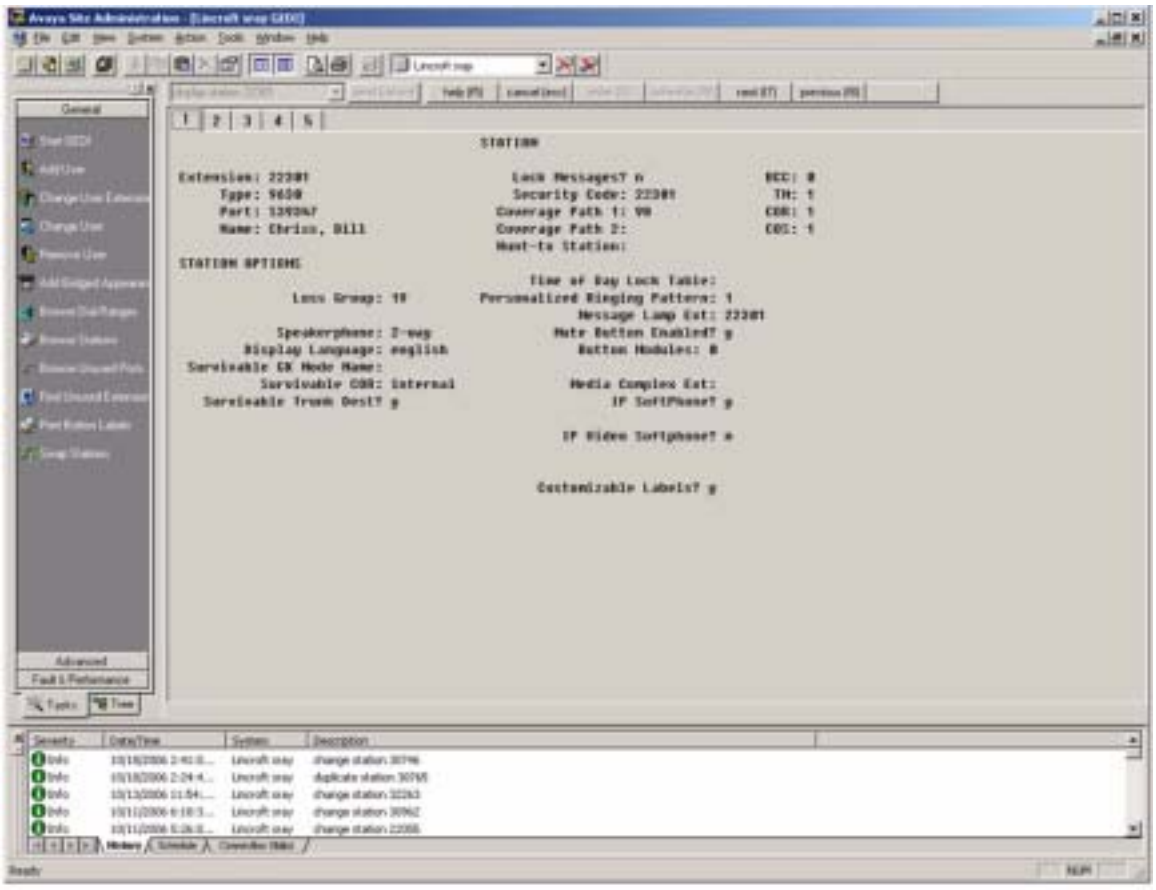


Figure 7: Station Form - Feature Options

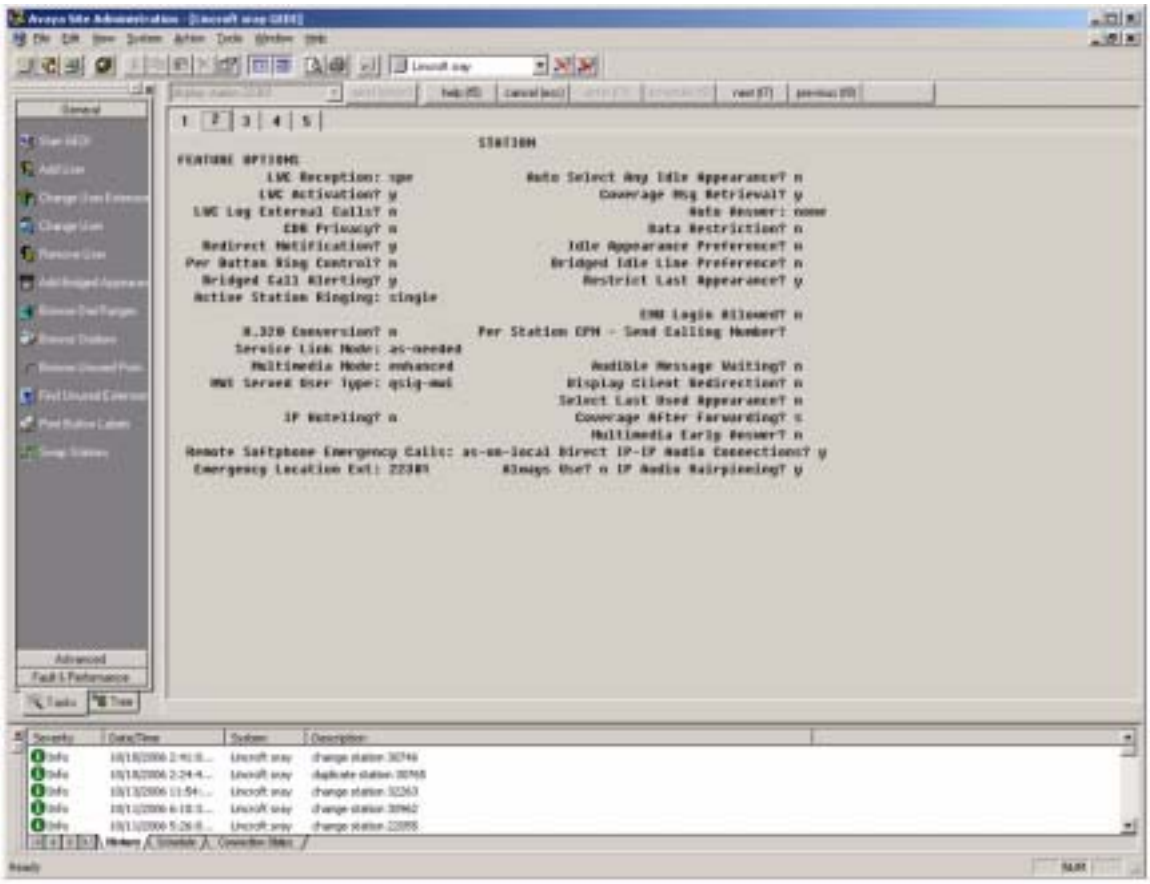

STATION
FEATURE OPTIONS
LWC Reception: spe
LWC Activation? y
LWC Log External Calls? n
CDR Privacy? n
Redirect Notification? y
Per Button Ring Control? n
Bridged Call Alerting? y
Active Station Ringing: single
H.320 Conversion? n
Service Link Mode: as-needed
Multimedia Mode: enhanced
MWI Served User Type: qsig-mwi
IP Hoteling? n
Remote Softphone Emergency Calls: as-on-local
Emergency Location Ext: 22389
Auto Select Any Idle Appearance? n
Coverage Msg Retrieval? y
Auto Answer: none
Data Restriction? n
Idle Appearance Preference? n
Bridged Idle Line Preference? n
Restrict Last Appearance? y
CWI Logic Allowed? n
Per Station CPN - Send Calling Number?
Audible Message Waiting? n
Display Client Redirection? n
Select Last Used Appearance? n
Coverage After Forwarding? s
Multimedia Early Answer? n
Direct IP-IP Audio Connections? y
Always Use? n IP Audio Hairpinning? y

Figure 8: Station Form - IP Phone Group ID, Bridged Calls, and Enhanced Call Forwarding

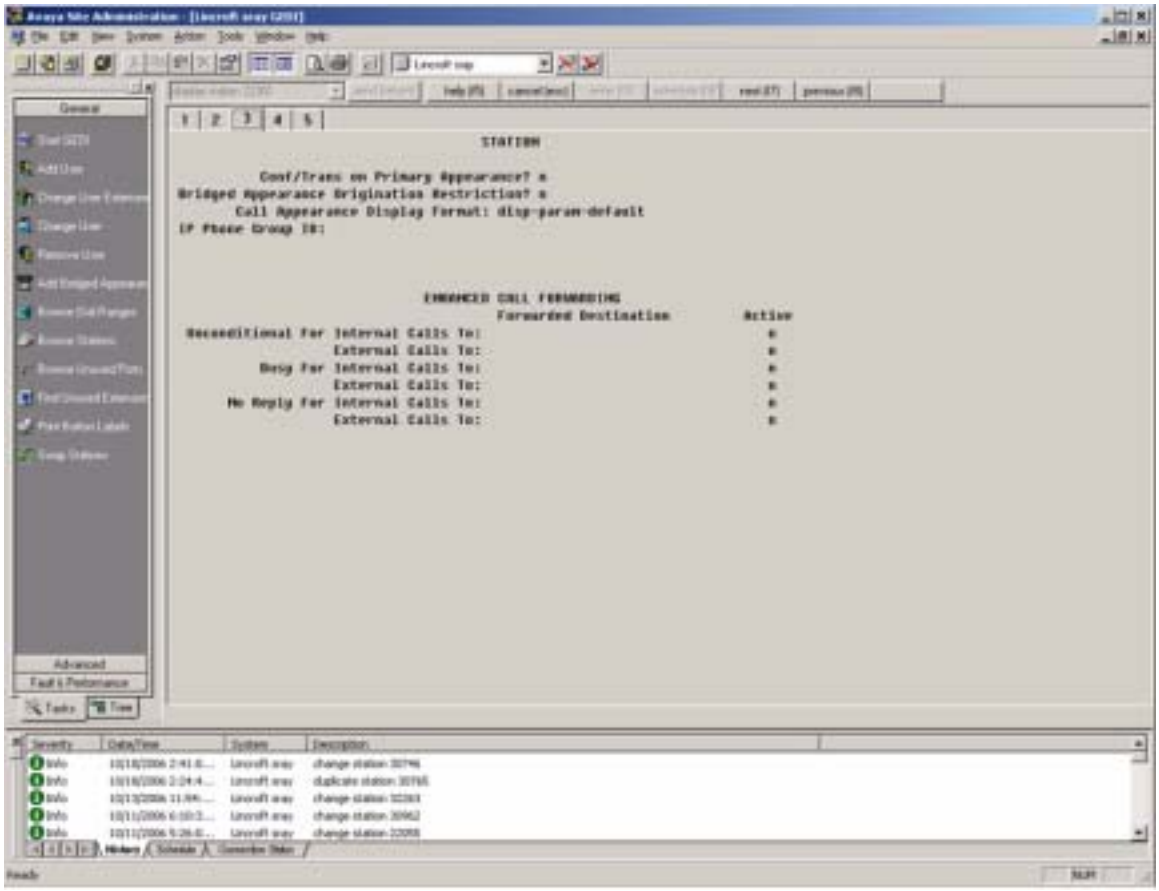


Figure 9: Station Form - Site Data, Abbreviated Dial, and Button Assignments

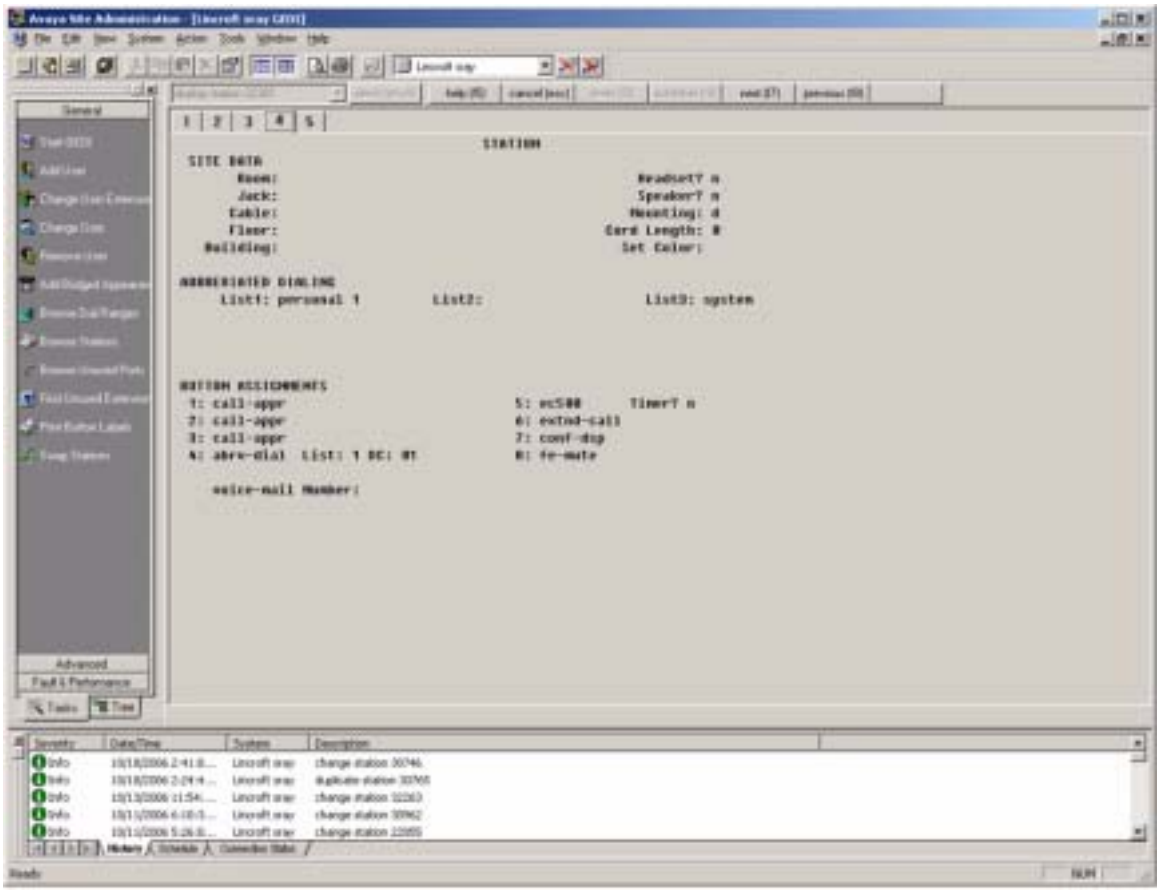


Figure 10: Feature-Related System Parameters Form

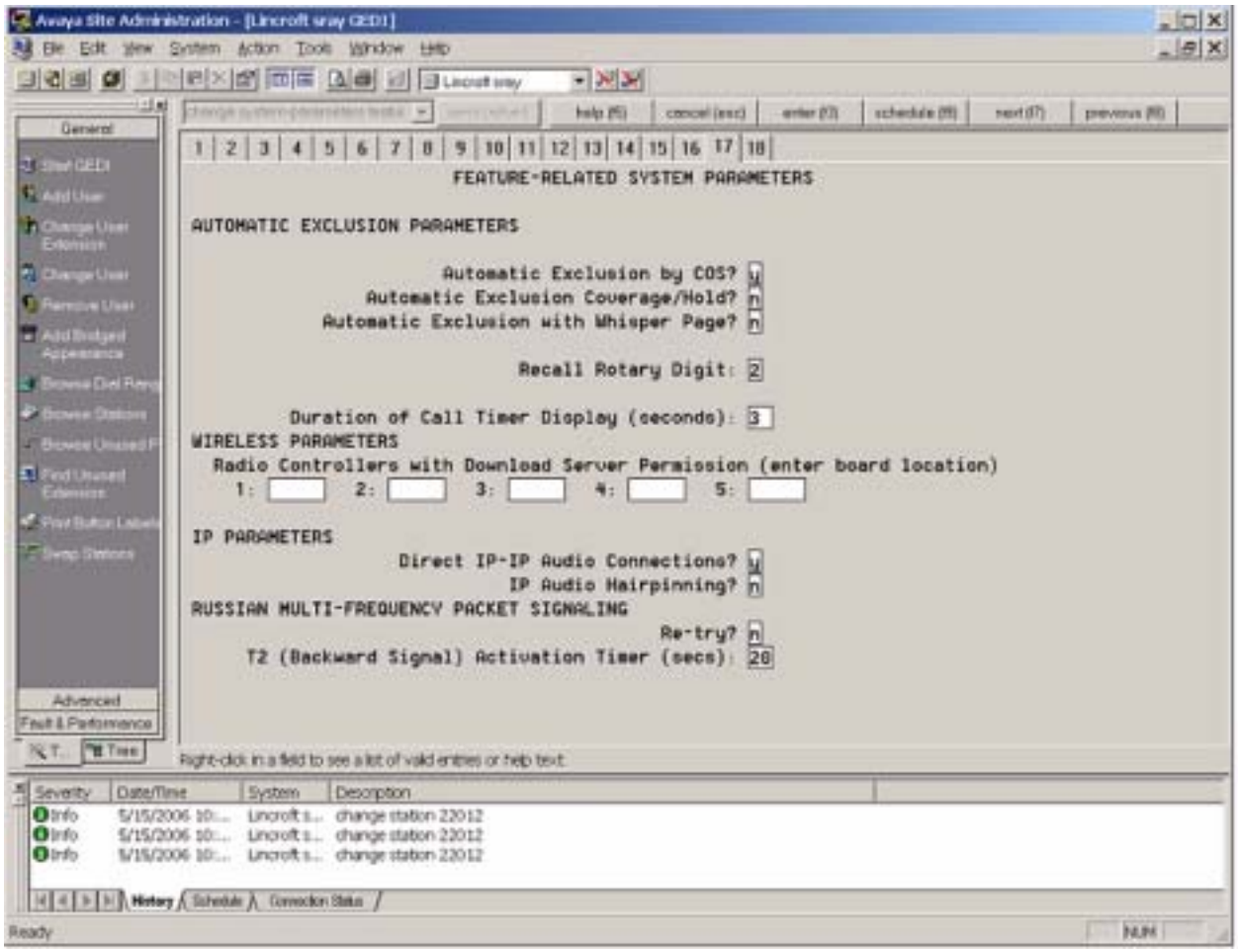

Avaya Site Administration - [Lincroft way CED1]
File Edit View System Action Tools Window Help
General
Advanced
Fault & Performance
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
FEATURE-RELATED SYSTEM PARAMETERS
AUTOMATIC EXCLUSION PARAMETERS
Automatic Exclusion by COS? y
Automatic Exclusion Coverage/Hold? n
Automatic Exclusion with Whisper Page? n
Recall Rotary Digit: 2
Duration of Call Timer Display (seconds): 3
WIRELESS PARAMETERS
Radio Controllers with Download Server Permission (enter board location)
1: 2: 3: 4: 5:
IP PARAMETERS
Direct IP-IP Audio Connections? y
IP Audio Hairpinning? n
RUSSIAN MULTI-FREQUENCY PACKET SIGNALING
Re-try? n
T2 (Backward Signal) Activation Timer (secs): 20
Right-click in a field to see a list of valid entries or help text
Severity Date/Time System Description
Info 5/15/2006 10:... Lincroft s... change station 22012
Info 5/15/2006 10:... Lincroft s... change station 22012
Info 5/15/2006 10:... Lincroft s... change station 22012
History Schedule Connection Status
Ready
NUM

Figure 11: IP Address Mapping Form

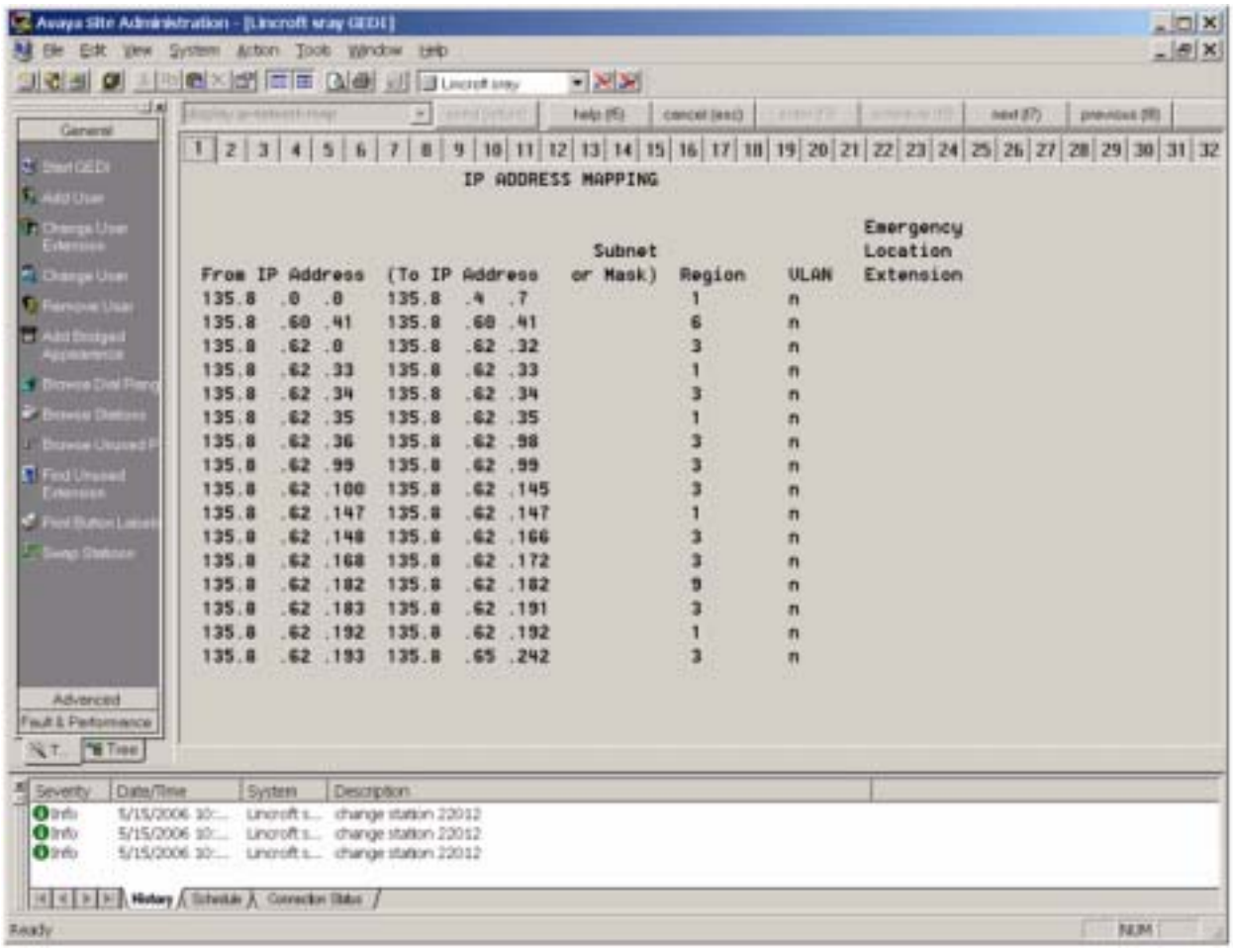


Figure 12: IP Codec Set Form

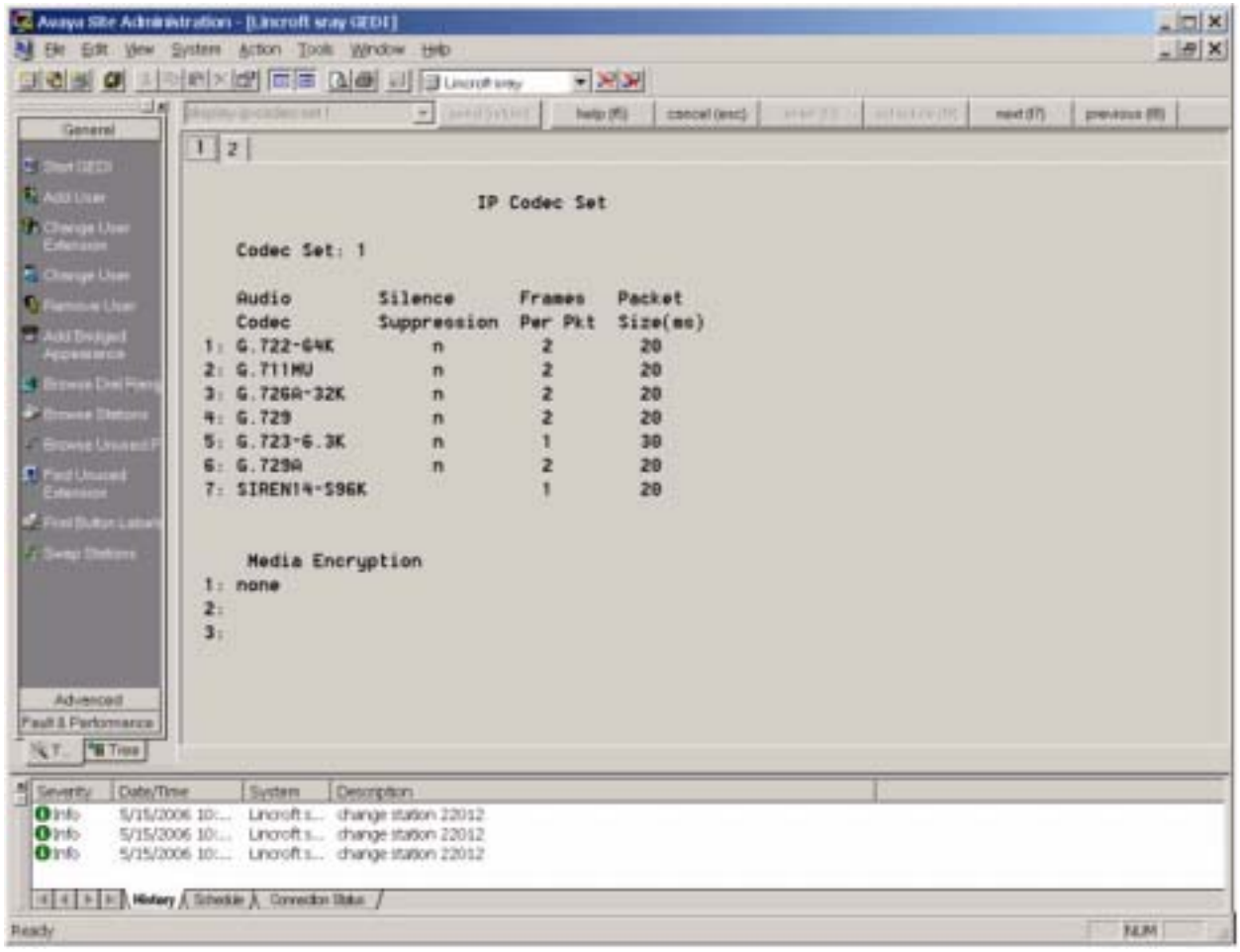
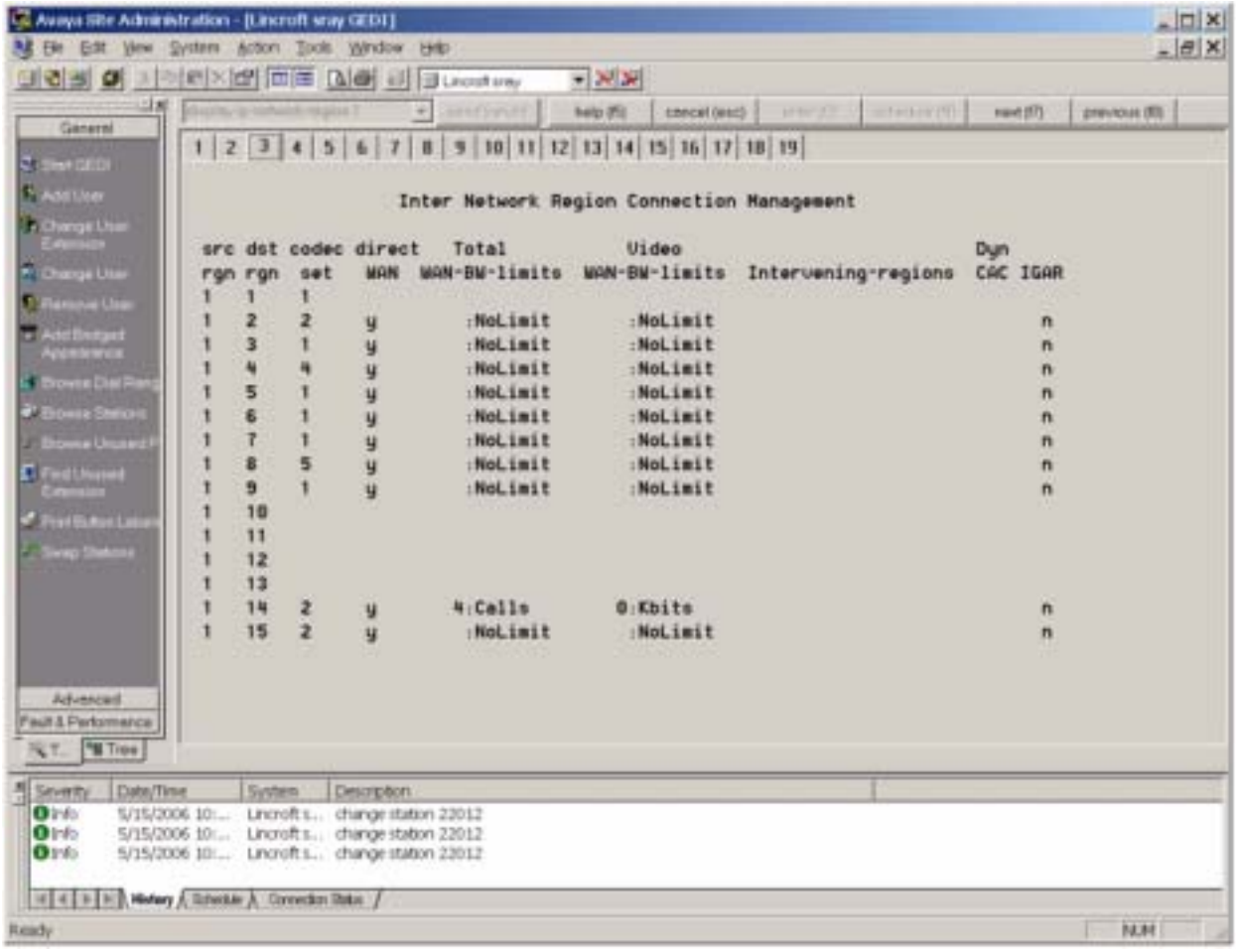


Figure 13: Inter-Network Region Connection Management Form


Inter Network Region Connection Management
src dst codec direct Total Video Dyn
rgn rgn set WAN WAN-BW-limits WAN-BW-limits Intervening-regions CAC IGAR
1 1 1
1 2 2 y :NoLimit :NoLimit n
1 3 1 y :NoLimit :NoLimit n
1 4 4 y :NoLimit :NoLimit n
1 5 1 y :NoLimit :NoLimit n
1 6 1 y :NoLimit :NoLimit n
1 7 1 y :NoLimit :NoLimit n
1 8 5 y :NoLimit :NoLimit n
1 9 1 y :NoLimit :NoLimit n
1 10
1 11
1 12
1 13
1 14 2 y 4:Calls 0:Kbits n
1 15 2 y :NoLimit :NoLimit n

The entries on the IP Address network map shown in Figure 11 might redirect endpoints into a particular network region. That region could be different from what is administered on the previous forms.

Figure 14: IP Network Region Form

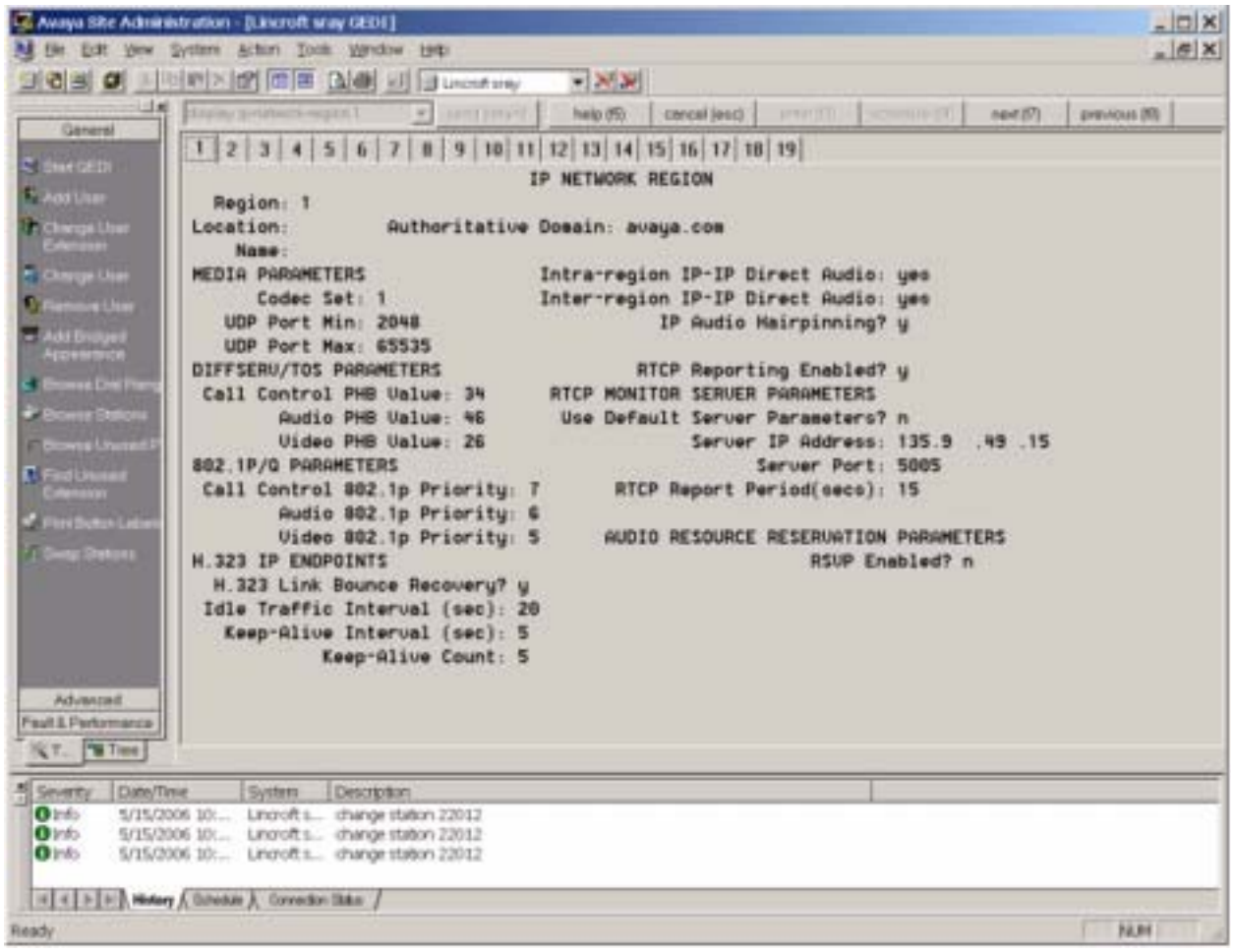
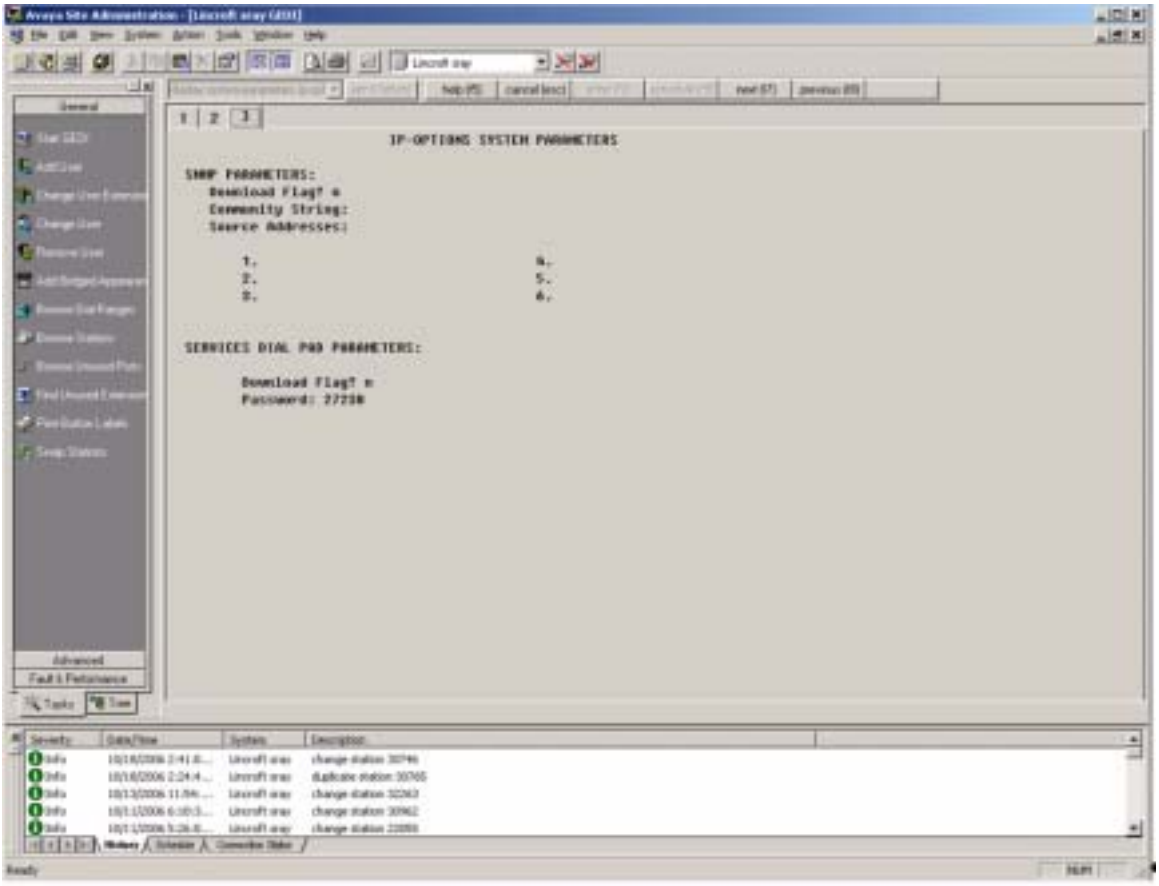


Figure 15: IP-Options System Parameters Form



Index

Numerical

802.1X . . . 104
9600 Series IP Telephones
- Administering Options for . . . 85
- Administration Alternatives and Options . . . 16
- Customizable System Parameters . . . 86
- Customizing Applications and Options . . . 137
- General . . . 15
- Initialization Process . . . 20
- Network Audio Quality Display . . . 28
- Scripts and Application Files . . . 80

9610 Craft Procedures . . . 173
9610 File Retrieval, General Processing . . . 134
9610 IP Telephone . . . 48
9610 IP Telephone, Special Administration for . . . 145
9610 IP Telephone, Troubleshooting . . . 173
9610 Key Administration Concepts . . . 168
9610 Restore File . . . 132
9610 Retrieval Procedures . . . 133
9620 IP Telephone . . . 49
9620, 9630/9630G, 9640/9640G, and 9650, Timer Operation . . . 160
9630, 9640, and 9650 IP Telephones . . . 49
9630/9630G and 9640/9640G IP Telephones, Enhanced Phone Screen Display . . . 51
9630/9630G, 9640/9640G, and 9650 Button Module (SBM24) . . . 51
9650 IP Telephone, Special Considerations . . . 52
9670 Home Screen, WML Application Display . . . 153
9670G Home Screen WML Application Icons/Labels . 153

A

About This Guide . . . 9
Ad-Hoc Conferences . . . 51
Administering Applications and Options . . . 137, 167
Administering Avaya Communication Manager . . . 37
Administering Features . . . 47
Administering Telephone Options . . . 85
Administration Alternatives and Options for 9600 Series IP Telephones . . . 16
Administration Forms . . . 185
Administration Forms, Samples . . . 185
Administration Overview and Requirements . . . 15
Administration, for Avaya Communication Manager . 37
Administration, for Telephones on call server . . . 44
Administrative Checklist . . . 19
Administrative Options, Local . . . 111
Administrative Process, The . . . 18
Aliasing . . . 37
Aliasing 9600 Series IP Telephones . . . 47
Alternatives, Administration . . . 16
ANSI/IEEE Documents . . . 183
Apache Web Servers, Configuring for Backup/Restore 77
Apache Web Servers, configuring for Backup/Restore 77
Application File and Upgrade Script, Choosing . . . 80
Application Files and Telephone Software . . . 79
Application Files, and Scripts for 9600 Series IP Telephones . . . 80
Application Icons/Labels, for 9670G Home Screen . 153
Application Status Flag (APPSTAT) . . . 144
Application Status Flags and Their Meaning . . . 144
Applications and Options, Administering . . . 137, 167
Applications, Customizing . . . 137
Application-specific parameters, administering . . . 17
APPSTAT . . . 144
Assessment, of Network . . . 23
Auto Hold administration . . . 45
Auto select any idle appearance administration . . . 48
Avaya "A" Menu Administration . . . 146
Avaya Menu Administration . . . 152
Avaya Menu Administration File Template . . . 158
Avaya Menu with WML Applications . . . 148

B

Backup . . . 129
Backup File Format, for the 9610 . . . 169
Backup File Formats . . . 129
Backup, Options and Non-Password Parameters Saved . . . 130
Backup/Restore . . . 127
Backup/Restore HTTP/HTTPS Configuration . . . 70
Backup/Restore, Configuring IIS Web Servers . . . 70
Button Module(s) (SBM24) . . . 51

C

Call Appearances and Feature Buttons . . . 48
Call Server (Switch) Administration . . . 38
Call Server Requirements . . . 37
Call Transfer Considerations . . . 42
Calltype Digit Analysis . . . 115
Checklist, Administrative . . . 19
Class of Restriction (COR) Form, Sample . . . 46
Codecs, Wide Band . . . 54
Communication Manager Administration . . . 37

Conference/Transfer on Primary Appearance administration 48
Conferencing Call Considerations 43
Contacts Application Administration, for the 9610 . . 171
Contacts File Format for USB Devices 162
Contents of the Settings File 82
Coverage Path administration 45, 48
Custom Screen Saver, Administering 126
Customizable System Parameters 86
Customizing 9600 Series IP Telephone Applications and Options 137

D

DHCP and File Servers 55
DHCP Generic Setup 27, 58
DHCP options 58
DHCP Parameters Set by 57
DHCP Server 24
DHCP Server Administration 56
DHCP Server Setup 56
DHCP Server to Telephone initialization 21
DHCP Server, Windows 2000 Setup 66
DHCP Server, Windows NT 4.0 Setup 63
DHCP, Configuring for 9600 Series IP Telephones . . 56
Dialing Methods 114
Dialing, Enhanced, Requirements 117
DIFFSERV 41
DNS Addressing 103
Document Organization 12
Documentation, Related 13, 183

E

EC500 administration 45
Enhanced Conference Features administration . . 45, 47
Enhanced Local Dialing 115
Enhanced Local Dialing Requirements 117
Enhanced Phone Screen Display for 9630/9630G and 9640/9640G IP Telephones 51
Error Conditions 22

F

Far End Mute administration 47
Feature Administration for Avaya Communication Manager 44
Feature Buttons and Call Appearances 48
Feature Numbers for Assigning Softkeys 120
Feature-Related System Parameters Form 189
Feature-Related System Parameters, administering on CM 44
Features, Administering 47
Features, Administering on Softkeys 117
File download
Choosing the Right Application and Upgrade Script File 80
Download File Content 80

G

General Download Process 79
Generic Setup, for DHCP 58
Gigabit Ethernet Adapter 114
Glossary of Terms 177
GROUP System Value 83
Guest User Administration 160

H

Hardware Requirements 23
HTTP/HTTPS Configuration for Backup/Restore . . . 70
HTTP/HTTPS Server 24

I

Idle Application 171
IEC/ISO Documents 183
IEEE 802.1D and 802.1Q 27, 40
IEEE 802.ID/Q QoS parameters 40
IEEE/ANSI Documents 183
IIS Web Servers, configuring for Backup/Restore . . . 70
Initialization Process, for 9600 Series IP Telephones . 20
Installation, Network Information Required before installing 25
Interface, administering the 17
Inter-Network Region Connection Management Form 192
IP Address Lists and Station Number Portability . . . 29
IP Address Mapping Form 190
IP Addresses, administering 16
IP Codec Set Form 191
IP Interface and Addresses, for call servers 39
IP-Options System Parameters Form 194
ISO/IEC, ANSI/IEEE Documents 183
ITU Documents 183

L

Language Selection 112
Link Layer Discovery Protocol (LLDP) 106
LLDP Data Units Transmitted 107
Local Administrative Options 111
Log Digit (Smart Enbloc) Dialing 115

M

Main Menu – No WML Applications 150
Main Menu (MM) Administration, for the 9610 . . . 170
Main Menu without WML Applications 150

N

NAT . . . 40
Network Assessment . . . 23
Network Audio Quality Display . . . 28
Network Considerations, Other . . . 26
Network Information, Required . . . 25
Network Region Form . . . 193
Network Requirements . . . 23

O

On-Hook Dialing administration . . . 44
OPSTAT . . . 93, 138, 147
Options and Applications, Administering . . . 137
Options, Administering . . . 85
Options, Customizing . . . 137
Options, entering using the Telephone Dialpad . . . 111
Options, for 9600 Series IP Telephone Administration 16
Other Considerations, for server administration . . . 41
Other Network Considerations . . . 26

P

Parameter Data Precedence . . . 18
Parameters in Real-Time . . . 28
Parameters Saved During Backup . . . 130
Parameters, Customizable . . . 86, 138
Pass-Through and Proxy Logoff, 802.1X . . . 105
Pictures, as screensaver . . . 164
Port Utilization
  Selection . . . 39
Processing, General, for 9610 Restore . . . 134
Proxy Logoff and Pass-Through, 802.1X . . . 105

Q

QoS . . . 27, 40
  Administrative Parameters . . . 17
  IEEE 802.1D and 802.1Q . . . 40
Qtest for Audio Quality . . . 28

R

Registration and Authentication . . . 34
Related Documentation . . . 183
Reliability and Performance . . . 27
Requirements . . . 15
  Call Server . . . 37
  Hardware . . . 23
  Network . . . 23
  Server . . . 24
Restore . . . 131
Restore File, for 9610 . . . 132
Restore/Backup . . . 127
Restrict Last Call Appearance administration . . . 48
Retrieval Procedures, for 9610 . . . 133
RSVP and RTCP . . . 39
RTCP and RSVP . . . 39

S

Sample Administration Forms . . . 185
Screen Saver, Administering . . . 126
Scripts and Application Files, for 9600 Series IP Telephones . . . 80
Security . . . 33
Send All Calls (SAC) administration . . . 47
Server Administration . . . 55
Server Administration, DHCP . . . 56
Server Administration, Other Considerations . . . 41
Server Requirements . . . 24
Settings File . . . 81
Settings File, Contents . . . 82
Shuffling Administration . . . 53
Smart Enbloc Dialing . . . 115
SNMP . . . 26
Softkeys, Administering Features on . . . 117
Software . . . 80
Software Checklist . . . 55
Software, Telephone . . . 80
SRTP . . . 31
Station Form
  Basic Telephone Information . . . 185
  Feature Options . . . 186
  IP Phone Group ID, Bridged Calls & Enhanced Call Forwarding . . . 187
  Site Data, Abbreviated Dialing, & Button Assignments . . . 188
Station Form - Basic Telephone Information . . . 185
Station Form - Feature Options . . . 186
Station Form Administration Results Chart . . . 49
Station Number Portability and IP Address Lists . . . 29
Supplicant Operation, 802.1X . . . 105
Switch Administration . . . 38
Switch Compatibility and Aliasing IP Telephones . . . 37
System Parameter Values, Impact of Received TLVs 109
System Parameters . . . 44
System Parameters, Customizable . . . 86, 138
System-Wide CM Administration . . . 44

T

Tagging and VLAN, administering . . . 16
TCP/UDP Port Utilization . . . 30
Telephone Administration . . . 16, 44
Telephone and Call Server initialization . . . 21
Telephone and File Server initialization . . . 21

Telephone Initialization Process 20
Telephone Options, Administering 85
Telephone Software and Application Files 79
Telephone to Network initialization 20
Terms, Glossary of 177
Timer Operation 160
Time-to-Service (TTS) 34
TLS 30
TLVs Received, Impact on System Parameter Values 109
Troubleshooting a 9610 IP Telephone 173

U

UDP Port Selection 39
UDP/TCP Port Utilization 30
Unnamed Registration 22
Upgrade Script and Application File, Choosing the Right 80
Upgrade Script File 80
Upgrade Script, contents of 82
USB Devices, Contacts File Format for 162
USB Devices, requirements for 162
USB Pictures 164

V

VLAN Considerations 100
VLAN Default Value 101
VLAN Detection 100
VLAN Separation 102
VLAN Separation Rules 102
VLAN Tagging 100
Voice Mail Integration 41
Voice-Initiated Dialing, Administering 113

W

Web Server 25
What's New 10
Wide Band Codecs 54
Wideband Audio administration 45
WML Application Display, on 9670G Home screen . . 153